ABSTRACT OF DOCUMENT (2)

INFORMATION PROCESSING SYSTEM AND TERMINAL DEVICE FOR WIDE-AREA NETWORK, AND USER IDENTIFICATION INFORMATION ENCRYPTING AND DECRYPTING METHODS

Publication number:	WO0195185
Publication date:	2001-12-13
Inventor:	NAKASHIMA KOUEI (JP)
Applicant:	NAKASHIMA KOUEI (JP)
Classification:	
- international:	***G06F21/00; G06Q20/00; H04L29/06;*** **G06F21/00; G06Q20/00; H04L29/06;** (IPC1-7): G06F17/60; G09C1/00; H04L9/00
- European:	G06F21/00N5A2D; G06Q20/00K2B; H04L29/06C6B; H04L29/06C6C2
Application number:	WO2001JP04717 20010604
Priority number(s):	JP20000167571 20000605; JP20000248499 20000818; JP20010068774 20010312

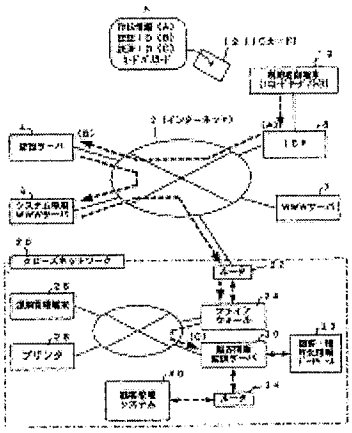
Cited documents:

- WO9608783
- JP10105614
- JP7141442
- JP11096363
- JP11203371

more >>

Abstract of **WO0195185**

An information processing system for providing a service to a user by utilizing a wide-area network, while preventing the information on the user from leaking reliably. An electronic settling system comprises an authentication server (4) and a dedicated WWW server (6) connected with the Internet (2) and a customer information conversion server (30) in a closed network (20) constructed in a financial institution or the like. A user terminal (10) can read information from an IC card (12) and is automatically connected with the WWW server (6) when the user connects the terminal with the WWW server (6) for Internet shopping, on the basis of the access information



and the authentication information in the IC card (12). When the user purchases a commodity, the settlement ID in the IC card (12) is transmitted for the settlement to a customer information conversion server (30). The settlement ID specifies the user, and all the customer information including the account number are stored in a database (32).

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年12 月13 日 (13.12.2001)

PCT

(10) 国際公開番号
WO 01/95185 A1

(51) 国際特許分類[7]: G06F 17/60, G09C 1/00, H04L 9/00

(21) 国際出願番号: PCT/JP01/04717

(22) 国際出願日: 2001 年6 月4 日 (04.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-167571 2000 年6 月5 日 (05.06.2000) JP
特願2000-248499 2000 年8 月18 日 (18.08.2000) JP
特願2001-068774 2001 年3 月12 日 (12.03.2001) JP

(71) 出願人 および
(72) 発明者: 中嶋公栄 (NAKASHIMA, Kouei) [JP/JP]; 〒462-0862 愛知県名古屋市北区真畔町48番地 Aichi (JP).

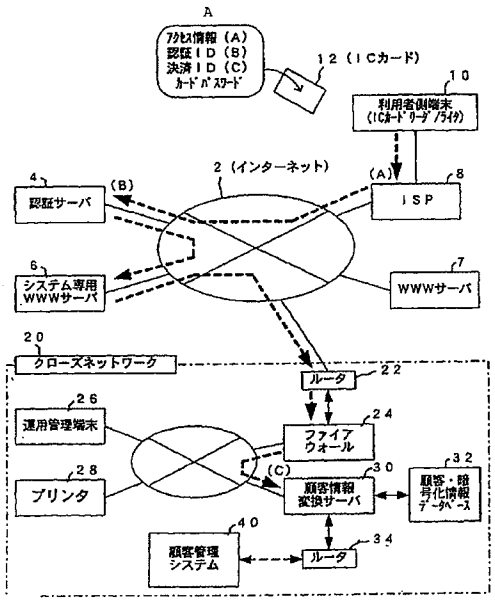
(74) 代理人: 弁理士 足立 勉(ADACHI, Tsutomu); 〒460-0003 愛知県名古屋市中区錦二丁目9番27号 名古屋繊維ビル7階 Aichi (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[続葉有]

(54) Title: INFORMATION PROCESSING SYSTEM AND TERMINAL DEVICE FOR WIDE-AREA NETWORK, AND USER IDENTIFICATION INFORMATION ENCRYPTING AND DECRYPTING METHODS

(54) 発明の名称: 広域ネットワーク用情報処理システム及び端末装置、並びに、利用者識別情報の暗号化方法及び暗号解読方法



28...PRINTER
30...CUSTOMER INFORMATION CONVERSION SERVER
32...CUSTOMER/ENCRYPTED INFORMATION DATABASE
34...ROUTER
40...CUSTOMER MANAGEMENT SYSTEM
A...ACCESS INFORMATION (A)
AUTHENTICATION ID (B)
SETTLEMENT ID (C)
CARD PASSWORD
2...(INTERNET)
4...AUTHENTICATION SERVER
6...SYSTEM DEDICATED WWW SERVER
7...WWW SERVER
10...USER TERMINAL (IC CARD READER/WRITER)
12...(IC CARD)
20...CLOSED NETWORK
22...ROUTER
24...FIRE WALL
26...OPERATION MANAGEMENT TERMINAL

(57) Abstract: An information processing system for providing a service to a user by utilizing a wide-area network, while preventing the information on the user from leaking reliably. An electronic settling system comprises an authentication server (4) and a dedicated WWW server (6) connected with the Internet (2) and a customer information conversion server (30) in a closed network (20) constructed in a financial institution or the like. A user terminal

[続葉有]

WO 01/95185 A1

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(10) can read information from an IC card (12) and is automatically connected with the WWW server (6) when the user connects the terminal with the WWW server (6) for Internet shopping, on the basis of the access information and the authentication information in the IC card (12). When the user purchases a commodity, the settlement ID in the IC card (12) is transmitted for the settlement to a customer information conversion server (30). The settlement ID specifies the user, and all the customer information including the account number are stored in a database (32).

(57) 要約:

広域ネットワークを利用して利用者個人に対するサービスを行う情報処理システムにおいて、利用者個人の情報が漏洩するのを確実に防止する。電子決済システムは、インターネット（２）に接続された認証サーバ（４）及び専用のＷＷＷサーバ（６）と、金融機関等に構築されたクローズネットワーク（２０）内の顧客情報変換サーバ（３０）とを備える。利用者側端末（１０）は、ＩＣカード（１２）から情報を読み取ることができ、利用者が専用ＷＷＷサーバ（６）に接続してインターネットショッピングを行う際には、ＩＣカード（１２）内のアクセス情報、認証情報に基づき、そのサーバに自動的に接続する。また利用者が商品を購入すると、ＩＣカード（１２）内の決済ＩＤが顧客情報変換サーバ（３０）に送信され、決済が行われる。決済ＩＤは、利用者を特定するためのものであり、口座番号等の顧客情報は、全てデータベース（３２）に格納されている。

明細書

広域ネットワーク用情報処理システム及び端末装置、並びに、利用者識別情報の暗号化方法及び暗号解読方法

技術分野

本発明は、インターネット等の広域ネットワークを利用して利用者に対するサービスを行うのに好適な広域ネットワーク用情報処理システム、及び、このシステムで利用するのに好適な端末装置、並びに、このシステムで利用者を特定するために利用される利用者の識別情報を暗号化するのに好適な決済用識別情報の暗号化方法及び暗号解読方法に関する。

背景技術

従来より、インターネット等の広域ネットワークを利用して、コンピュータプログラム，楽音データといった情報や各種物品を販売する所謂オンラインショッピングが知られている。

ところで、こうしたオンラインショッピング用のシステムでは、料金を利用者から安全に徴収できるように、通常、商品等の情報を提供する要求受付手段（一般に販売用ホームページを開設するＷＷＷサーバ）とは別に、購入要求の意志表示をした利用者が信頼できるものであるか否かを判定して利用者が信頼できる場合にのみその利用者への販売を許可し、その利用者から料金を徴収するための決済処理を行う情報処理装置が設置されている。

そして、こうした情報処理装置にて決済処理を行うには、利用者から徴収すべき料金や販売内容等を表す料金情報だけでなく、利用者の特定・信用調査等を行うのに必要な利用者個人の情報や、決済に必要な金

融機関の口座番号・クレジットカード番号等の決済用情報が必要である。このため、従来では、通常、利用者側端末との間で直接通信を行う要求受付手段が、広域ネットワークを介して利用者側端末から利用者個人の決済用情報を取得し、その取得した決済用情報を料金情報と共に情報処理装置に転送するようにしていた。

しかしながら、こうした決済のために、従来のように、利用者個人の決済用情報を広域ネットワークを介して取得するようにすると、これらの情報がそのまま広域ネットワーク上に流れることになるので、決済用情報が第三者に流れ、悪用されることが考えられる。

一方、こうした問題に鑑み、従来では、決済用情報を暗号化して送信したり、或いは、決済用情報だけは電話回線等の専用の通信回線を使って送信することにより、決済用情報が第三者に漏洩して悪用されるのを防止している。

しかし、決済用情報を単に暗号化したのでは、暗号化に使った鍵を取得すれば簡単に解読できることから、決済用情報の漏洩を確実に防止することはできない。また、決済用情報を専用の通信回線を使って送信するようにした場合には、利用者側端末に、広域ネットワークへの接続回路と、専用の通信回線への接続回路とを設けなければならず、利用者側端末のコストアップを招き、利用者の金銭的負担が大きくなり、延いては、利用者にとって利用し難いものとなってしまう。

また、上記従来のシステムでは、利用者がオンラインショッピング等で所望の商品を購入する意思表示をすると、ＷＷＷサーバ等の要求受付手段が、決済用情報の入力書式を利用者側端末に送信し、利用者は、その送信されてきた入力書式に従い、決済用情報を入力して、広域ネットワーク上に送信する必要があったことから、利用者にとって使い勝手が悪いという問題もあった。

また、こうした利用者の個人情報の漏洩は、広域ネットワークを利用して電子決済を行うシステム以外でも同様に起こる。

例えば、利用者個人の健康状態や各種医療機関での診療状態等の健康管理データをデータベース化し、これを広域ネットワークを利用して、個人や各種医療機関が利用できるようにした場合、健康管理データの登録・検索の際には、個人を特定する情報（名前・電話番号等）もネットワーク上に流れることになるが、これらの情報が第三者に渡ると、データベースへの不正アクセスが可能となり、利用者個人の健康管理データが公表されてしまうとから、健康管理データが改竄されてしまう、といった問題が発生する。

発明の開示

本発明は、こうした問題に鑑みなされたもので、広域ネットワークを利用して利用者個人に対するサービスを行う情報処理システムにおいて、利用者個人の情報が漏洩するのを確実に防止し、利用者が安心して利用できるようにすることを目的とする。

かかる目的を達成するためになされた請求項１記載の広域ネットワーク用情報処理システムにおいては、要求受付手段が、広域ネットワークを介して利用者側端末との間で通信を行い、利用者側端末から当該システムで提供可能なサービスの要求（例えば、上述した商取引のための決済要求、個人情報の更新・検索の要求等）を受け付ける処理を実行する。そして、要求受付手段は、利用者側端末から実際にサービスの要求を受けると、利用者側端末から、利用者を特定するために暗号化された識別情報を取得し、これを利用者が要求してきたサービスを表す情報と共に、情報処理手段に送信する。

すると、情報処理手段は、その識別情報を解読し、解読後の識別情報

を、予め利用者毎に顧客情報が登録されている顧客情報データベースと照合することにより、利用者が予め登録された顧客であるか否か（換言すれば、利用者がサービスを享受可能な顧客であるか否か）を判断し、利用者がサービスを享受可能な顧客であれば、顧客情報データベースに登録された顧客情報に基づき、利用者が要求してきたサービスを実現するための情報処理を行う。

つまり、本発明では、利用者にサービスを提供するのに必要な顧客情報を利用者毎に登録した顧客情報データベースを予め作成しておき、利用者が実際にサービスを享受する際には、利用者側端末から要求受付手段に、利用者を特定するための識別情報を暗号化して送信するようにしている。

従って、本発明によれば、広域ネットワーク上に、利用者から要求されたサービスを提供するのに必要な顧客情報（例えば、利用者の氏名、住所、口座番号、…といった個人情報）を送信する必要がなく、当該システムで利用者を特定し得る識別情報のみを流せばよいので、利用者個人の顧客情報が第三者に渡って悪用されるのを防止できる。

また、情報処理手段は、要求受付手段から入力される識別情報と利用者が要求してきたサービスの内容を表す情報を受け取って、予め顧客として登録された利用者に対するサービスを行うようにされており、この情報処理手段と広域ネットワークとの間の通信経路は、要求受付手段によって遮断されていることから、情報処理手段に対する外部からの不正アクセスを確実に防止し、顧客情報が不正アクセスによって外部に流出するのを防止できる。

また、要求受付手段は、利用者の識別情報と利用者が要求してきたサービスの内容を表す情報を情報処理手段に入力するだけであり、情報処理手段から要求受付手段へと顧客情報が伝送されることはないことから、

これによっても、顧客情報が外部に流出するのを防止できる。

よって、本発明によれば、利用者にとって安心して利用できるサービス提供システムを構築ききる。

ところで、本発明の広域ネットワーク用情報処理システムでは、利用者側端末から暗号化した識別情報を広域ネットワーク上に送信し、これを広域ネットワーク上の要求受付手段が取得して、更に情報処理手段に転送することにより、情報処理手段が、その識別情報を元に利用者を特定して、利用者が要求してきたサービスのための情報処理を行うことになるが、第三者が、利用者側端末から広域ネットワーク上に送信された全情報情報を取得し、これをそのまま使用することにより、当該システムに侵入することも考えられる。そこで、こうしたことをより確実に防止するには、当該システムを請求項２に記載のように構成するとよい。

即ち、請求項２に記載のシステムにおいては、要求受付手段が、利用者側端末から識別情報を取得する際、利用者側端末に対して、識別情報と共に識別情報に対応したパスワードを送信するよう要求する。すると、この要求を受けた利用者側端末は、利用者に対して、識別情報に対応したパスワードの入力を要求し、この要求に応じて利用者が入力してきたパスワードと識別情報とを要求受付手段に送信し、要求受付手段は、その送信されてきた識別情報及びパスワードを情報処理手段に転送する。そして、情報処理手段は、要求受付手段から送信されてきた識別情報とパスワードとに基づき利用者が顧客であるか否かを判定する。

従って、請求項２記載のシステムによれば、パスワードを知らない第三者は、利用者の識別情報を取得しても、本発明の広域ネットワーク用情報処理システムに侵入することができなくなり、安全性をより向上することが可能となる。

次に請求項３に記載の広域ネットワーク用情報処理システムは、本発

明（請求項１，２）を、利用者に対するサービスとして、ネットワーク上の商取引の際に必要になる決済処理を行うシステムに適用したものであり、情報処理手段として、顧客情報データベースを用いて得られる顧客情報（決済に必要な金融機関の口座番号やクレジットカード番号等）に基づき、利用者から料金を徴収するための決済処理を行う決済手段を備える。

そして、要求受付手段は、利用者側端末からの要求に従い、当該システムで実現可能な商取引のための情報（例えば、インターネットショッピングのためのホームページ等）を提供し、その情報提供の結果、利用者側端末から商取引のための決済要求を受けると、利用者から徴収すべき料金を表す料金情報を、利用者側端末から取得した識別情報と共に、決済手段に転送する。

従って、請求項３に記載のシステムによれば、広域ネットワークを利用した商取引を実現するために、決済に必要な利用者の顧客情報（金融機関の口座番号やクレジットカード番号等）をネットワーク上に流す必要がなく、利用者を特定する識別情報のみを流せばよいので、利用者の金融機関の口座番号やクレジットカード番号が第三者に渡って、利用者が金銭的被害に遭うのを防止できる。

また、利用者がネットワーク上で商取引を行うためのホームページを開設しているサイトは、多数存在するが、請求項３に記載のシステム（所謂電子決済システム）は、こうした既存のサイトを、要求受付手段として機能させることにより、容易に実現できる。

そして、この場合、決済処理を行う決済手段（情報処理手段）を金融機関等に構築することで、要求受付手段としての機能を有するサイトと決済手段（情報処理手段）とを分離しておけば、要求受付手段（サイト）を開設している情報提供者が利用者の顧客情報を取得することができな

くなるので、情報提供者が利用者の顧客情報を悪用するといったことも防止でき、利用者にとって安心して利用できる商取引用のシステムを構築できる。

ところで、請求項３に記載のシステムにおいて、情報処理手段は、要求受付手段から転送されてきた識別情報を解読することにより利用者を特定し、その利用者が、顧客情報データベースに顧客情報が登録された利用者である場合に、料金徴収のための決済処理を行うが、より確実に決済処理を行うためには、顧客情報に基づき実際に決済をできるかどうかを確認できることが望ましい。

そして、このためには、請求項４記載のように、決済手段を、顧客情報データベースに基づき利用者が予め登録された顧客であると判定すると、外部（例えば金融機関や信用調査機関）の信用調査用データベースに接続して、利用者の信用調査を行い、信用調査の結果、利用者は信用できると判定した場合にのみ決済処理を行い、利用者は信用できないと判定した際には、要求受付手段に対してその利用者との間の商取引を中止させるように構成するとよい。

また、請求項３又は４に記載のシステムにおいて、決済手段としては、銀行やクレジットカード会社等の金融機関の管理コンピュータに直接接続して、その金融機関から直接料金を徴収するように構成してもよく、或いは、請求項５に記載のように、デビットカード決済センター等の外部の料金徴収システムに対して、利用者及び徴収金額を表す情報を送信することにより、外部の料金徴収システムを介して決済処理を行うようにしてもよい。

一方、請求項３～請求項５に記載のシステムは、商品の販売若しくは各種サービスを行う各種販売会社が個々に構築することができるが、各販売会社がこのシステムを個々に構築すると、複数の販売会社を利用し

たい利用者は、各販売会社毎に識別情報等を管理しなければならず、その管理が極めて面倒になる。

そこで、本発明を適用した請求項３～請求項５に記載のシステム（電子決済システム）を実際に構築する場合には、請求項６に記載のように、当該システムを、各種販売会社からの委託を受けて利用者との間で商取引を行う販売代行会社にて管理するようにすればよい。尚、この場合、要求受付手段は、情報処理手段としての決済手段にて利用者から料金を徴収可能であると判定された際に、その利用者との間の商取引の結果を、対応する販売会社に通知するように構成する必要はある。

そして、このように、要求受付手段及び決済手段（情報処理手段）を全て販売代行会社にて管理し、成立した商取引の結果だけを販売会社に通知するようにすれば、利用者は、販売代行会社に登録した一つの識別情報を用いて複数の販売会社から所望の商品を購入したり或いは所望のサービスを受けることができるようになり、利用者の利便性を向上できる。

また、販売会社は、販売業務を販売代行会社へ委託するだけで、広域ネットワークを使った商品販売若しくはサービスの受注を行うことができる。よって販売会社にとっては、広域ネットワークを使った商取引に必要な設備投資が不要となり、販売代行会社へ手数料を支払うだけで、販路を容易に拡大することができるようになる。

一方、複数の販売会社を利用する利用者側で識別情報の管理を簡単に行えるようにするには、請求項７に記載のように、請求項３～請求項５に記載のシステムにおいて、要求受付手段を、利用者との間で商取引を行う販売会社にて管理し、決済手段（情報処理手段）を、販売会社からの委託を受けて決済処理を行う決済代行会社にて管理するようにしてもよい。

つまり、このようにした場合、商品販売や各種サービスを行う販売会社側で要求受付手段を管理する必要があるものの、識別情報から利用者を特定する情報処理手段は、その販売会社から委託を受けた決済代行会社側で管理されるので、利用者は、その決済代行会社に一つの識別情報を登録しておけばよく、識別情報の管理を容易に行うことができるようになる。

よって、請求項７に記載のシステムにおいても、利用者の利便性を向上できる。また、この場合、販売会社は、決済に必要な利用者の顧客情報を管理する必要がないので、システムの運用を容易に行うことができ、しかも、利用者は、顧客情報を販売会社に知られることがないので、当該決済システムを安心して利用できる。

一方、請求項８に記載の広域ネットワーク用情報処理システムは、本発明（請求項１，２）を、利用者個人の個人情報（換言すればプライベート情報）を管理する所謂データベースシステムに適用したものであり、情報処理手段として、顧客情報データベースを用いて得られる顧客情報に関連づけて利用者個人の個人情報が記憶された個人情報データベースを備え、要求受付手段を介して、顧客情報データベースに登録された顧客本人から個人情報の登録若しくは検索要求があると、その要求に従い個人情報データベースに登録された顧客本人の個人情報を更新若しくは検索する個人情報管理手段を備える。

そして、要求受付手段は、利用者側端末から個人情報データベースに登録された個人情報の更新若しくは検索要求を受けると、その個人情報の更新若しくは検索要求を、利用者側端末から取得した識別情報と共に、個人情報管理手段に転送する。

つまり、請求項８に記載のシステムは、利用者の個人情報（プライベート情報）を管理し、利用者からの要求に従い、個人情報の更新若しく

は検索を行うものであるが、利用者が個人情報の更新若しくは検索を行う際に利用者側端末からネットワーク上に送信されるのは、識別情報と更新若しくは検索の要求だけであることから、利用者のプライベート情報が第三者に渡って、利用者が被害を受けるのを防止できる。

また、例えば、利用者が個人情報を更新する際に、利用者側端末から更新データを送信するようにしても、その更新データに付与されるのは、当該システムで利用者を識別するための識別情報であり、利用者を特定可能な顧客情報（この場合、利用者の住所・電話番号・連絡先等）は送信されないことから、第三者が更新用データを不正に取得したとしても、その更新用データが誰のものかを特定することができず、更新データの流出によって利用者が被害を受けるのを防止できる。

尚、利用者が個人情報の検索要求を行った場合、検索結果をネットワークを介してそのまま利用者側端末に送信するようにすると、その送信先から、利用者が特定されてしまう虞があるので、このような場合は、専用の通信回線若しくはセキュリティ保護された専用のホームページ等を利用して、検索結果を送信するようにすればよい。

ここで、請求項８に記載のシステムにおいて、個人情報データベースに登録する利用者個人の個人情報（プライベート情報）としては、例えば、利用者の資産、経歴、趣味等に関するあらゆる情報を挙げることができるが、特に、請求項９に記載のように、個人情報として、利用者個人の健康状態を表す情報を個人情報データベースに登録するようにすれば、利用者個人が自己の健康状態を把握し、健康管理に気を付けることになるので、利用者にとって極めて有効なシステムとなりうる。

また、この場合、利用者の健康状態を表す個人情報として、利用者側端末に設けた測定器（所謂バイタル測定器）を使って、利用者の現在の生体特性（脈拍、血圧、体脂肪、酸素、二酸化炭素、血流、血液、髪の

毛、爪、口内皮膜、口内粘膜、唾液等）を測定し、これを毎日、個人情報データベースに登録するようにすれば、利用者が病気になった際に、その蓄積した個人情報を医師に提示することにより、より適切な診断を受けることができるようになる。

また、この場合、例えば、情報処理手段としての個人情報管理手段側で、個人情報データベースに蓄積されたデータから、利用者毎に健康状態を判断し、その判断結果を、個人情報データベースに書き込む、診断処理を定期的に実行するようにすれば、利用者は、その診断結果から、自己の健康状態を判断できるようになる。尚、この場合、診断結果を電子メール等で利用者個人に直接配信するようにしてもよい。

また次に、請求項８又は請求項９に記載のシステムにおいては、個人情報データベース内の利用者毎の個人情報を、各利用者毎に予め許可された個人が検索若しくは更新できるようにしてもよい。

そして、このためには、請求項１０に記載のように、個人情報管理手段に、個人情報データベースに登録された個人情報を更新若しくは検索可能な利用者本人以外の者が顧客情報に関連付けて記憶された個人情報利用者データベースを設け、要求受付手段を介して、顧客情報データベースに登録された顧客から他人の個人情報の更新若しくは検索要求が入力された際には、個人情報管理手段が、個人情報利用者データベースを参照して、個人情報の更新若しくは検索要求を行った顧客が更新若しくは検索可能な個人情報を抽出し、その抽出した個人情報に対する更新若しくは検索処理を行うようにするとよい。

つまり、このようにすれば、例えば、個人情報データベースに蓄積される個人情報が利用者の資産に関する情報である場合に、これを、利用者が契約している弁護士や税理士等に公開することで、利用者は、これらの者に資産管理を任せ、必要に応じてチェックすることができるよう

になる。

また、特に、請求項９に記載のように、個人情報データベースに、利用者個人の健康状態を表す情報を登録するようにした場合には、請求項１１に記載のように、その個人情報を医師や薬剤師が検索・更新できるように、個人情報利用者データベースに利用者が指定した医師若しくは薬剤師を登録するようにするとよい。

そして、この場合には、個人情報データベースに登録される利用者個人の個人情報（健康状態を表す情報）を、医師がチェックして、利用者に対して、適切なアドバイスを行うようにすることができるし、また、医師が、カルテを個人情報データベースに書き込めるようにすることにより、診察時に、過去の診療履歴と利用者（患者）の現在の健康状態とを利用して、より効率よく適切な診断を下すことができる。

また、個人情報データベースに薬剤師がアクセスして、利用者（患者）がそのとき服用している薬剤をチェックしたり、書き込むことができるようにすれば、異なる薬剤師による薬剤の二重投与を防止することができる。また、この場合、医師は、薬剤の投与によって利用者の健康状態がどのように変化したかを監視し、より適切な診療を行うことができる。

一方、本発明（請求項１～請求項１１）の広域ネットワーク用情報処理システムにおいて、要求受付手段との間で通信を行う利用者側端末としては、広域ネットワークに接続可能な端末装置であればよいが、どのような端末装置でも要求受付手段にアクセスできるようにすると、上述した顧客情報（或いは顧客情報及び顧客個人のプライベート情報）の秘匿性を確保できなくなることも考えられる。

そこで、こうした顧客情報等の秘匿性をより向上するには、請求項１２に記載のように、認証手段を設け、認証手段が、要求受付手段にサービスの要求をしてきた利用者側端末から広域ネットワークを介して認証

情報を取得し、その認証情報が予め登録された利用者のものであるときに、利用者側端末と要求受付手段との通信を許可するようにするとよい。

つまり、このようにすれば、要求受付手段にアクセス可能な端末装置を、認証手段に予め登録された特定の利用者だけに制限することができる。そして、この場合、要求受付手段に対してサービスを要求できるのは、認証手段に予め登録された特定の利用者だけであるので、顧客情報等の秘匿性を向上できる。

ところで、本発明（請求項１～請求項１２）の広域ネットワーク用情報処理システムでは、利用者側端末からサービスの要求と共に送信すべき情報は利用者の識別情報だけであり、顧客情報を送信する必要はないため、従来のように、サービスを要求する度に、利用者が顧客情報を入力する必要がない。このため、本発明によれば、利用者によるデータ入力を少なくし、利用者側端末の操作性を向上できる。

しかしながら、本発明の広域ネットワーク用情報処理システムにおいて、利用者がサービスを享受するには、利用者側端末から識別情報を送信する必要があり（請求項１～請求項１１）、場合によっては、更に、要求受付手段への接続用の認証情報を送信する必要がある(請求項１２)。そして、こうした識別情報や認証情報を、サービスを要求する度に利用者が入力するようにした場合には、折角、顧客情報の入力を省略できるようになったにも係わらず、利用者にとっては、煩わしい操作を強いられることになる。

また、利用者側端末から送信する識別情報は、安全のために暗号化されるが、利用者が識別情報を入力するようにすると、識別情報の暗号化を利用者側端末で行わなければならず、このためには、利用者側端末内に暗号化のための鍵を記憶しておかなければならない。そして、このように利用者側端末内に暗号化鍵を記憶するようにすると、第三者が利用

者側端末を不正に操作して、システムへの不正アクセスを行うことができるようになるし、また、暗号化鍵が第三者に盗まれてしまう虞もある。

そこで、こうした問題を防止して、システムのセキュリティ性をより高めるには、利用者側端末を請求項１３又は請求項１４に記載のように構成するとよい。

即ち、請求項１３に記載の発明は、請求項１～請求項１１の何れかに記載の広域ネットワーク用情報処理システムにおいて、利用者側端末として使用される端末装置に関するものであり、暗号化された識別情報が記憶された記憶媒体を着脱自在に装着でき、しかも、その装着された記憶媒体から情報を読み取るための情報読取手段を備える。そして、この端末装置は、要求受付手段から識別情報の要求があると、その要求された情報を情報読取装置を介して記憶媒体から自動で読み出し、広域ネットワーク上に送出する。

従って、請求項１３に記載の端末装置によれば、請求項１～請求項１１の何れか記載の広域ネットワーク用情報処理システムで利用することにより、端末装置を要求受付手段に接続したり、サービスの要求を送信したりする際に、利用者自らが識別情報を入力する必要がなく、操作性を向上することができる。また、利用者は、これらの識別情報を記憶した記憶媒体を保管しておけば第三者に不正使用されるのを防止できることから、安全性をより向上することができる。

また、請求項１４に記載の発明は、請求項１２に記載の広域ネットワーク用情報処理システムにおいて、利用者側端末として使用される端末装置に関するものであり、要求受付手段に接続するための利用者の認証情報と識別情報とが記憶された記憶媒体を着脱自在に装着でき、しかも、その装着された記憶媒体から各情報を読み取るための情報読取手段を備える。そして、この端末装置は、認証手段又は要求受付手段から認証情

報又は識別情報の要求があると、その要求された情報を情報読取装置を介して記憶媒体から自動で読み出し、広域ネットワーク上に送出する。

従って、この請求項１４に記載の端末装置によれば、請求項１２に記載の広域ネットワーク用情報処理システムで利用することにより、端末装置を要求受付手段に接続したり、サービスの要求を送信したりする際に、利用者自らが認証情報や識別情報を入力する必要がなく、操作性を向上することができる。また、利用者は、これらの情報を記憶した記憶媒体を保管しておけば第三者に不正使用されるのを防止できることから、安全性をより向上することができる。

尚、利用者が本発明のシステムを利用する際には、利用者側端末（端末装置）を広域ネットワークに接続する必要があるが、請求項１５に記載のように、上記請求項１３又は請求項１４に記載の端末装置において、識別情報（若しくは識別情報及び認証情報）を記憶した記憶媒体に、更に、広域ネットワークへの接続情報を記憶しておき、端末装置自体が、記憶媒体から読み出した接続情報に基づき自動で広域ネットワークに接続するように構成すれば、利用者の使い勝手をより向上することができる。

また、上記のように記憶媒体に識別情報、認証情報認、接続情報等を記憶するようにした場合、利用者が記憶媒体を保管していれば、第三者による不正使用を防止することはできるが、紛失・盗難等により記憶媒体が第三者にわたると、第三者は、この記憶媒体を使って不正なサービスを享受できるようになる。

そこで、請求項１６に記載のように、請求項１３～請求項１５に記載の端末装置において、記憶媒体には、予めパスワードを設定しておき、端末装置自体を、情報読取手段に記憶媒体が装着された際に利用者に対してパスワードの入力を要求し、そのパスワードが設定されたものと不

一致であるときには、要求受付手段への接続を禁止するように構成するとよい。

またこの場合、更に請求項１７に記載のように、端末装置を、入力されたパスワードが設定されたものと不一致であることを所定回数連続して判定した際に、記憶媒体を使用不能にするように構成すれば、第三者による不正使用をより確実に防止できる。

尚、こうした端末装置による記憶媒体のパスワード判定動作は、予め利用者側端末に登録したプログラムにより実現されるように構成してもよく、或いは、記憶媒体内にパスワード判定用のプログラムを記憶しておき、端末装置がそのプログラムを実行することによりパスワード判定動作を実現するようにしてもよい。

また、請求項１２に記載のシステムで利用される請求項１４に記載の端末装置に、請求項１６或いは請求項１７に記載の発明を適用した場合には、パスワードが設定されたものと一致しているか否かの判定を、端末装置ではなく、認証手段側で実行するようにしてもよい。つまり、利用者が入力してきたパスワードと認証情報とを、端末装置側から広域ネットワークを介して認証手段に送信し、認証手段側で、そのパスワードが認証情報と共に予め登録されたパスワードと一致しているか否かを判定して、その判定結果を利用者側端末に送信するようにしてもよい。

尚、請求項１６又は請求項１７に記載の端末装置で、第三者による端末装置の不正使用を判定するのに用いるパスワードは、請求項２に記載のシステムにおいて、要求受付手段からの要求に応じて利用者側端末が要求受付手段に送信するパスワードと兼用することができる。

一方、上記のように記憶媒体の不正使用を防止するには、請求項１８に記載のように、記憶媒体に、予め利用者の指紋情報を記憶しておき、情報読取手段に記憶媒体が装着されると、端末装置が、端末に備えられ

た指紋センサを介して利用者の指紋を検出し、その検出結果と記憶媒体に記憶された指紋情報とから利用者の指紋が記憶媒体に登録された指紋情報と一致するか否かを判定し、不一致であるときに、要求受付手段への接続を禁止するようにしてもよい。

またこの場合、利用者は、端末装置に設けられた指紋センサに指紋を読み取らせる必要があるが、請求項１９に記載のように、端末装置に設けられた操作用のリモートコントロール装置（以下、リモコン装置という）に指紋センサを組み込むようにすれば、指紋入力を端末本体から離れた位置で簡単に行うことができるので、便利である。

尚、このように指紋情報を用いて利用者を特定する場合の判定動作は、上述したパスワードの判定動作と同様、予め端末装置に登録したプログラムにより実現されるように構成してもよく、或いは、記憶媒体内に指紋判定用のプログラムを記憶しておき、端末装置がそのプログラムを実行することにより実現するようにしてもよい。

また、端末装置に、音声認識装置とこれに音声を入力するためのマイクロフォン（以下、マイクという）とを設けて、利用者を特定するようにしても、記憶媒体の不正使用を防止することはできる。つまり、端末装置を利用する際には、マイクから所定の音声を入力するようにし、音声認識装置が、マイクから入力された音声信号を分析して、分析により得られた声紋等の特徴パラメータから利用者を認識して、要求受付手段への接続を許可するようにしてもよい。

また次に、記憶媒体としては、少なくとも、利用者の認証情報や識別情報といった各種情報を記憶できればよいため、読取専用の記憶媒体であってもよいが、より好ましくは、情報の書き換え若しくは追加書き込みができる記憶媒体とするとよい。つまり、このようにすれば、記憶した情報の更新等を行うことができ、記憶媒体自体の使い勝手を向上でき

る。また記憶媒体は、利用者が保管しやすいように、キャッシュカードやクレジットカード等と同じカード状にすることが望ましい。

そして、このためには、記憶媒体としては、一般的な磁気カードにて構成してもよいが、特に、情報の書き換えを行ったり、或いは、上述したプログラムの書き込み等により書き込むべき情報量が多い場合には、請求項２０に記載のように、記憶媒体をＩＣカードにて構成し、端末装置には、情報読取手段としてＩＣカードリーダ／ライタを設けるようにするとよい。

尚、端末装置自体は、ＩＣカードリーダ／ライタ等からなる情報読取手段を、インターネット等の広域ネットワークへの接続機能を有する汎用のパーソナルコンピュータに組み込むことにより構成し、端末装置としての機能を、パーソナルコンピュータが実行するプログラムにて実現するようにしてもよく、或いは、ＩＣカードリーダ／ライタ等からなる情報読取手段を搭載した専用の端末装置にて実現するようにしてもよい。

また、端末装置としての機能を、例えば、パーソナルコンピュータ，携帯電話等の情報機器、テレビゲーム機，テレビ等の家電製品、自動車用ナビゲーション装置等の車載機器、に組み込み、利用者が、これらの情報機器、家電製品若しくは車載機器を操作することにより、当該システムを利用できるようにしてもよい。

次に、請求項２１記載の発明は、上述した本発明（請求項１～請求項１２）の広域ネットワーク用情報処理システムにおいて、利用者側端末から広域ネットワークを介して要求受付手段に送信される識別情報の暗号化方法に関するものである。

そして、この暗号化方法では、まず、暗号化前の識別情報を、識別情報を構成する文字や記号或いは文字列からなる語句データに区分し、その語句データ毎に、予め作成された登録語句置換シートを用いて符号化

し、その後、符号化した語句データを、予め作成された乱数シートに記述された乱数を用いて所定データ長の暗号化データに変換し、その変換後の暗号化データを順に配置することにより、暗号化した識別情報を生成する。

つまり、請求項２１記載の暗号化方法では、暗号化鍵として、登録語句置換シートと乱数シートとの二つの鍵を利用し、識別情報を二段階で暗号化する。この結果、暗号化された識別情報を解読するには、暗号化に用いた２つの鍵（登録語句置換シート及び乱数シート）を用いて、２段階に復号化する必要がある。

よって、本発明方法によれば、上述した本発明（請求項１～請求項１２）のシステムにおいて、利用者側端末から広域ネットワーク上に送出される識別情報を第三者が取得しても、その識別情報を解読することは困難となり、識別情報の秘匿性を確保できる。

また、請求項２２記載の暗号化方法では、上記のように識別情報を暗号化するのに使用する２つの鍵（登録語句置換シート及び乱数シート）のうちの少なくとも一方を、所定期間毎に更新し、暗号化した識別情報に、その鍵の種別を表す種別情報を付与する。

このため、本発明方法によれば、上述した本発明（請求項１～請求項１２）のシステムにおいて、識別情報を解読する鍵（登録語句置換シート及び乱数シート）を入手した者が、広域ネットワークから識別情報を取得したとしても、その鍵を使って識別情報を解読できる確率は極めて低くなり、識別情報の秘匿性をより向上することができる。

一方、請求項２３記載の発明は、本発明（請求項１～請求項１２）の広域ネットワーク用情報処理システムにおいて、情報処理手段が暗号化された識別情報を解読して利用者を特定するのに好適な暗号解読方法に関するものである。

そして、この解読方法では、まず、暗号化された識別情報を、所定データ長の暗号化データに区分し、各暗号化データ毎に、前記識別情報を暗号化した際に用いられた乱数シートに記述された乱数を用いて、符号化された語句データに変換し、その後、変換後の語句データを、識別情報を暗号化した際に用いられた登録語句置換シートを用いて、暗号化前の識別情報を構成する文字、記号又は文字列からなる語句データに変換し、その変換後の語句データを順に配置することにより、暗号化前の識別情報を復元する。

よって本発明方法によれば、上述した本発明（請求項１～請求項１２）のシステムにおいて、利用者側端末から広域ネットワーク上に送出する識別情報を請求項２１又は請求項２２記載の暗号化方法で暗号化するようにし、情報処理手段側で、その暗号化された識別情報を解読する際に、本発明方法を用いるようにすることで、情報処理手段側で識別情報を確実に解読することができるようになる。

図面の簡単な説明

図１は、実施例の電子決済システムの概略構成を表すブロック図であり、

図２は、利用者側端末にて実行される制御処理を表すフローチャートであり、

図３は、認証サーバにて実行される制御処理を表すフローチャートであり、

図４は、システム専用のＷＷＷサーバにて実行される制御処理を表すフローチャートであり、

図５は、顧客情報変換サーバにて実行される制御処理を表すフローチャートであり、

図６Ａ，Ｂ，Ｃ，Ｄは、決済ＩＤの暗号化及び暗号解読に用いられる登録語句置換シート及び乱数シートのデータ構成並びにこれを用いた暗号化手順及び解読手順を説明する説明図であり、

図７Ａ，Ｂは、決済ＩＤの暗号化及び暗号解読の手順を表すフローチャートであり、

図８は、実施例の電子決済システムを適用した通信販売システム（ａ）の構成を表すブロック図であり、

図９は、実施例の電子決済システムを適用した通信販売システム（ｂ）の構成を表すブロック図であり、

図１０は、操作用のリモコン装置を備えた利用者側端末の構成例を表すブロック図であり、

図１１は、図１０の利用者側端末において利用者を識別するために端末本体及びリモコン装置にて実行される処理を表すフローチャートであり、

図１２は、第２実施例の電子決済システムの概略構成を表すブロック図であり、

図１３は、第２実施例の電子決済システムにおいてデビットカードによる決済を行う際に各サーバで実行される処理を表すフローチャートであり、

図１４は、第３実施例の健康管理システムの概略構成を表すブロック図であり、

図１５は、第３実施例の利用者側端末、専用ＷＷＷサーバ、顧客情報変換サーバにて実行される個人情報の登録・閲覧手順を表すフローチャートであり、そして

図１６は、第３実施例の個人情報管理サーバにて実行される個人情報管理処理を表すフローチャートである。

発明を実施するための最良の形態

以下に本発明の実施例を図面と共に説明する。

［第１実施例］

図１は本発明（詳しくは請求項３～請求項７）が適用された第１実施例の電子決済システム全体の構成を表すブロック図である。

図１に示すように、本実施例の電子決済システムは、広域ネットワークとしてのインターネット２に接続された認証サーバ４、及び、当該システム専用のＷＷＷ（World Wide Web）サーバ（以下、専用ＷＷＷサーバという）６と、銀行，クレジットカード会社等に構築されたクローズネットワーク２０内の顧客情報変換サーバ３０とを備える。

認証サーバ４は、ＩＳＰ（Internet Service Provider ）を介してインターネット２に接続された端末装置としての利用者側端末１０から認証情報（以下、認証ＩＤという）を取得し、この認証ＩＤに基づき、現在この利用者側端末１０を操作している利用者は予め当該システムの利用者として登録されているか否かを判定して、利用者が登録されている場合にだけ、利用者側端末１０の専用ＷＷＷサーバ６への接続を許可し、利用者側端末１０の接続先を専用ＷＷＷサーバ６へ誘導するものであり、本発明の認証手段に相当する。

専用ＷＷＷサーバ６は、認証サーバ４により接続が許可された利用者側端末１０からの要求に従い、オンラインショッピング等の商取引のための情報を提供すると共に、利用者側端末１０との間で商取引のための通信を行うものであり、本発明の要求受付手段に相当する。

また、専用ＷＷＷサーバ６は、利用者側端末１０との間で行う商取引のための通信の結果、利用者から商品の購入代金等の料金を徴収する必要がある場合には、利用者側端末１０から、決済用の暗号化された識別

情報（以下、決済ＩＤという）を取得し、取得した決済ＩＤと、利用者が購入しようとする物品若しくは情報の種別や金額等を表す料金情報とを、インターネット２を介して、クローズネットワーク２０内の顧客情報変換サーバ３０に送信する。

そして、その情報の送信の結果、顧客情報変換サーバ３０側から送信されてくる決済結果に従い、決済できた否かを判定し、決済できた場合には、利用者に対する商品の配送（商品が情報であれば送信）を行い、決済できなければ、その利用者への商品の販売を中止する。

一方、顧客情報変換サーバ３０が接続されたクローズネットワーク２０は、ファイアウォール２４及びルータ２２を介してインターネット２に接続されており、顧客情報変換サーバ３０は、専用ＷＷＷサーバ６からインターネット２を介して料金情報及び決済ＩＤが送信されてくると、その決済ＩＤに基づき利用者を特定して、その利用者の口座から料金を引き落とすための決済処理を実行する。つまり、顧客情報変換サーバ３０は、本発明の情報処理手段として機能する。

また、顧客情報変換サーバ３０には、専用ＷＷＷサーバ６から送信されてきた暗号化された決済ＩＤを解読するのに必要な暗号化情報（鍵）や、解読した決済ＩＤから利用者を特定して、利用者の口座番号やクレジットカード番号といった決済用の顧客情報を取得するための顧客・暗号化情報データベース３２が接続されている。そして、顧客情報変換サーバ３０は、この顧客・暗号化情報データベース３２を用いて、決済ＩＤを解読すると共に、その解読した決済ＩＤに対応した顧客情報を取得することにより、料金徴収用の決済処理を行う。

尚、クローズネットワーク２０には、ファイアウォール２４や顧客情報変換サーバ３０以外に、本実施例の電子決済システムを運用・管理するための運用管理端末２６、各種情報を印刷するためのプリンタ２８と

いった、各種情報処理用の端末装置が接続されている。また、顧客情報変換サーバ３０には、ルータ３４を介して、銀行，クレジットカード会社等で顧客管理システム４０を構築しているネットワークに接続されており、顧客情報変換サーバ３０は、この顧客管理システム４０内の信用調査用データベースを利用して利用者の信用調査を行う。

また次に、利用者側端末１０には、キーボードやマウスといった入力装置や、専用ＷＷＷサーバ６から提供される商品購入のための情報や各種操作用の情報を表示するための表示装置が設けられている。この結果、利用者は、表示装置に表示される画面に従い入力装置を操作することにより、購入物品を選択したり、選択した物品の購入（決済）を指令できる。

また、利用者側端末１０には、本発明の情報読取手段として、ＩＣカードリーダ／ライタが設けられている。そして、利用者側端末１０は、このＩＣカードリーダ／ライタに、上述した認証ＩＤや決済ＩＤが記憶されたＩＣカード１２が装着されるか、或いは、ＩＣカード１２が装着されている状態で利用者からインターネット２への接続指令が入力されると、ＩＳＰ８を介して自動的にインターネット２に接続し、認証サーバ４に対して専用ＷＷＷサーバ６への接続要求を送信する。

またＩＣカード１２には、上述した認証ＩＤ及び決済ＩＤに加えて、利用者が加入しているＩＳＰ８へのアクセス情報（請求項７記載の接続情報）も記憶されており、利用者側端末１０は、インターネット２への接続時には、ＩＣカード１２からアクセス情報を読み出し、この情報に基づき、ＩＳＰ８，延いてはインターネット２に接続する。

尚、利用者側端末１０とＩＳＰ８とを接続するには、利用者側端末１０にＩＳＰ８に接続するための通信手段を設ける必要があるが、この通信手段としては、一般的な公衆電話回線網（アナログ回線若しくはデジ

タル回線）を使ってＩＳＰに接続するための電話用通信装置（モデムやターミナルアダプタ等）であってもよく、携帯電話，ＰＨＳといった無線電話を使ってＩＳＰに接続するための無線電話用通信装置であってもよく、或いは、ＣＡＴＶを利用してＩＳＰに接続するための通信装置（所謂ケーブルモデム）であってもよい。また、近年、通信衛星を使ってインターネットサービスを行うＩＳＰや、専用の通信線を使ってインターネットサービスを行うＩＳＰも実用化されつつあるが、こうしたＩＳＰを利用するのであれば、利用者側端末１０には、ＩＳＰ接続用の通信手段として、衛星通信用のアンテナ（パラボラアンテナ，平面アンテナ等）を介して通信衛星との間で通信を行うための衛星通信装置や、ＩＳＰとの間で専用の通信線を介して通信を行うための専用の通信装置を設ければよい。また、携帯電話等の携帯型通信装置信端末にＩＣカードリーダ／ライタを内蔵又は外付けすることにより、利用者側端末１０自体を、携帯電話等の携帯型通信装置にて構成してもよい。

次に、上記のように構成された構成された本実施例の電子決済システムにおいて、利用者が実際にインターネットショッピングを行う際のデータの流れを説明する。

まず、利用者が本実施例の電子決済システムを利用するために、ＩＣカード１２を利用者側端末１０に装着するか、或いは、ＩＣカード１２を利用者側端末１０に装着した状態でインターネット２への接続指令を入力すると、利用者側端末１０は、ＩＣカード１２からインターネット２へのアクセス情報を読み出し、その読み出したアクセス情報に基づき、ＩＳＰ８にインターネット２への接続要求を送信する（図１に点線で示す矢印（Ａ）参照）。

そして、この接続要求の送信によって、利用者側端末１０がＩＳＰ８を介してインターネット２に接続されると、図１に矢印（Ｂ）で示すよ

うに、利用者側端末１０から認証サーバ４に、ＩＣカード１２に記憶された認証ＩＤが送信される。すると、認証サーバ４では、その認証ＩＤに基づき、利用者は当該システムを利用するために予め登録された者であるかどうかを判定し、この判定により利用者が認証されると、利用者側端末１０が、認証サーバ４を介して、専用ＷＷＷサーバ６に接続される。

そして、このように利用者側端末１０が専用ＷＷＷサーバ６に接続されると、専用ＷＷＷサーバ６から利用者側端末１０に、インターネットショッピング等のための情報が送信され、利用者側端末１０の表示装置にその情報が表示されることから、利用者は、表示画面を見ながら利用者側端末１０を操作することにより、所望の商品を選択して、購入することができるようになる。

またこの状態で、利用者が所望の商品を購入するために、キーボードの所定の購入決定キーを押下するか、或いはマウスで表示画面上の購入決定用ボタンをクリックすることにより、選択した商品の購入決定を表す情報を専用ＷＷＷサーバ６に送信すると、専用ＷＷＷサーバ６から利用者側端末１０に対して決済ＩＤを要求する情報が送信される。

すると、利用者側端末１０は、ＩＣカード１２から決済ＩＤを読み出し、専用ＷＷＷサーバ６に送信する。また、専用ＷＷＷサーバ６側では、決済ＩＤを受信すると、これに、利用者が購入を決定した商品の種別や購入金額を表す料金情報を付与して、クローズネットワーク２０内の顧客情報変換サーバ３０に送信することから、図１に矢印（Ｃ）で示すように、決済ＩＤは、最終的には、顧客情報変換サーバ３０まで伝送されることになる。

そして、顧客情報変換サーバ３０では、決済ＩＤを受信すると、これを、顧客・暗号化情報データベース３２内の暗号化情報を用いて解読す

ることにより、利用者を特定し、更に、顧客・暗号化情報データベース３２を検索することにより、この利用者の顧客情報を、顧客・暗号化情報データベース３２から抽出する。

また、顧客情報変換サーバ３０では、受信した決済ＩＤから利用者を特定して顧客情報を抽出できた場合には、顧客管理システム４０側の信用調査用データベースを使って、利用者の信用調査を行い、信用調査の結果、利用者は商品を購入できると判断すると、料金情報及び顧客情報を顧客管理システム４０に送信することにより、利用者の口座から購入代金を引き落とすための決済処理を行い、その決済結果を専用ＷＷＷサーバ６に送信し、専用ＷＷＷサーバ６は、この決済結果を利用者側端末１０に転送する。

尚、顧客情報変換サーバ３０は、受信した決済ＩＤを解読することにより利用者を特定できない場合や、顧客情報を抽出できない場合、或いは、信用調査の結果、利用者は商品を購入することができないと判断した場合は、決済結果として、その旨を表す情報を専用ＷＷＷサーバ６に送信し、専用ＷＷＷサーバ６は、この決済結果についても、利用者側端末１０に転送する。

次に、こうしたデータの流れ（換言すれば当該システム全体の動作）を実現するために、利用者側端末１０、認証サーバ４、専用ＷＷＷサーバ６、顧客情報変換サーバ３０にて各々実行される制御処理について説明する。

まず図２は、利用者側端末１０で実行される制御処理を表すフローチャートである。

図２に示すように、利用者側端末１０では、Ｓ１１０（Ｓはステップを表す）にてＩＣカードリーダ／ライタにＩＣカード１２が装着されたか否かを判定することにより、ＩＣカード１２が装着されるのを待ち、

ＩＣカード１２が装着されると、Ｓ１２０にて、利用者からインターネット２への接続指令が入力されたか否かを判断することにより、利用者から接続指令が入力されるのを待つ。尚、Ｓ１２０では、Ｓ１１０にて最初にＩＣカード１２が装着されたと判断された直後には、接続指令が入力されたものと判断する。

そして、Ｓ１２０にて、利用者からインターネット２への接続指令が入力されたと判断されると、Ｓ１３０にて、表示装置に、ＩＣカード１２を使用するために予め設定されたパスワードの入力画面を表示し、利用者からのパスワードの入力を受け付ける、パスワード受付処理を実行する。そして、利用者が表示画面に従いＩＣカード１２のパスワードを入力すると、続くＳ１４０にて、その入力されたパスワードは、ＩＣカード１２に予め登録（記憶）されているパスワードと一致するか否かを判定し、パスワードが一致しなければ、パスワードが誤入力されたと判断して、Ｓ１５０に移行する。

Ｓ１５０では、パスワードが連続して何回誤入力されたかを判定できるようにするために、パスワードの誤入力があった旨を表す情報（日時等）をＩＣカード１２に書き込むと共に、ＩＣカード１２に書き込まれた過去の情報から、誤入力の連続回数を求め、連続誤入力回数が予め設定された上限値（例えば７回）に達したか否かを判定し、更に、連続誤入力回数が上限値に達していれば、その後、そのＩＣカード１２を使用できないように、ＩＣカード１２を使用禁止情報を書き込む、誤入力達続回数判定処理を実行する。そして、この処理終了後は、再度Ｓ１１０に移行する。

一方、Ｓ１４０にて、利用者が入力したパスワードとＩＣカード１２に登録されたパスワードとが一致していると判断されると、Ｓ１６０に移行し、ＩＣカード１２からインターネット２へのアクセス情報を読み

込み、その読み込んだアクセス情報に従い、ＩＳＰ８にインターネット２への接続要求を送信することにより、当該利用者側端末１０をＩＳＰ８を介してインターネット２に接続させる。

尚、Ｓ１６０では、ＩＣカード１２にインターネット２に接続した旨を表す情報（日時等）を書き込む。この結果、Ｓ１５０にて、ＩＣカード１２に書き込まれた過去の情報（使用履歴）から、誤入力の連続回数を正確に判定できることになる。

次に、Ｓ１６０の処理により、当該利用者側端末１０がインターネット２に接続されると、今度は、Ｓ１７０にて、ＩＣカード１２から認証ＩＤを読み出し、これをインターネット２上の認証サーバ４に送信する。すると、認証サーバ４側では、送信した認証ＩＤに基づき当該利用者側端末１０がシステムを利用可能であるか否かを判定する認証ＩＤ判定処理が実行され、その判定結果（認証結果）を、当該利用者側端末１０に送信してくるので、続くＳ１８０では、その認証結果を受信し、受信した認証結果を表示装置に表示する。

またこうして、Ｓ１８０にて認証結果が受信されると、今度は、Ｓ１９０にて、受信した認証結果に基づき、当該利用者側端末１０は認証サーバ４側で認証されたか否かを判定する。そして、認証サーバ４側で認証されていなければ、専用ＷＷＷサーバ６に接続できないことから、再度Ｓ１１０に移行し、逆に、認証サーバ４側で認証された場合には、続くＳ２００に移行する。

Ｓ２００では、使用者からの指令、若しくは、認証サーバ４からの指令により、認証ＩＤやＩＣカード１２のパスワードといった認証データを更新する必要があるか否かを判断する。そして、認証データの更新が必要であれば、Ｓ２１０にて、認証サーバ４からＩＣカード１２の認証データ書込ロックを解除するための情報を取得して、ＩＣカード１２の

認証データ書込ロックを解除し、続くＳ２２０にて、ＩＣカード１２内の認証データを、使用者が入力してきた新たな認証データ、若しくは、認証サーバ４から送信されてきた新たな認証データに書き換える認証データの更新処理を実行する。また、この認証データ更新処理実行後は、ＩＣカード１２内の認証データを勝手に書き換えることができないようにするために、認証データ書込ロック用の情報を認証サーバ４から取得し、この情報を用いて、ＩＣカード１２に対して、認証データ書込ロックを設定する。

つまり、ＩＣカード１２に記憶される認証ＩＤやパスワードを簡単に書き換えることができると、第三者によるＩＣカード１２の不正使用を防止できないことから、本実施例では、こうした認証データは、認証サーバ４側の監視の下に更新でき、認証サーバ４が許可しない限り認証データを更新できないようにしているのである。尚、これらの認証データと同様、ＩＣカード１２に記憶される決済ＩＤについても、書込ロックが設定されていることは言うまでもない。

次に、Ｓ２００にて、認証データを更新する必要はないと判断されるか、Ｓ２１０～Ｓ２３０の認証データ更新のための処理が実行されると、今度は、Ｓ２４０に移行して、当該利用者側端末１０を専用ＷＷＷサーバ６に接続する。尚、この接続は、認証サーバ４から送信されてくる情報に基づき、自動で実行される。

そして、その後は、Ｓ２５０にて、利用者からの指令に従い、専用ＷＷＷサーバ６や専用ＷＷＷサーバ６からアクセス可能な他のＷＷＷサーバ７（図１参照）との間で通信を行う、一般的なインターネットアクセス処理を実行する。

また、このアクセス処理実行時には、周期的に下記の処理を実行することにより、インターネット２への接続を遮断したり、専用ＷＷＷサー

バ６を利用したインターネットショッピングによる商品購入のための処理を実行する。

即ち、Ｓ２６０では、利用者からインターネット２との接続を遮断する指令（接続遮断指令）が入力されたか否かを判断し、接続遮断指令が入力された場合には、Ｓ３２０で、インターネット２への接続を遮断した後、Ｓ１１０に移行する。

また、Ｓ２６０にて、接続遮断指令が入力されていないと判断すると、Ｓ２７０に移行して、インターネットアクセス処理実行時に利用者が所望商品の購入指令を入力したことに伴い専用ＷＷＷサーバ６から決済ＩＤの要求があったか否かを判断する。そして、決済ＩＤの要求がなければ、再度Ｓ２５０に移行し、決済ＩＤの要求があれば、Ｓ２６０に移行して、表示装置に、決済用のパスワードの入力画面を表示し、利用者からのパスワードの入力を受け付ける、決済用のパスワード受付処理を実行する。

そして、利用者が表示画面に従い決済用のパスワードを入力すると、続くＳ２９０に移行して、ＩＣカード１２から決済ＩＤを読み出し、その読み出した決済ＩＤと決済用のパスワードとを、専用ＷＷＷサーバ６に送信する。

すると、専用ＷＷＷサーバ６は、これらの情報を料金情報と共に顧客情報変換サーバ３０に送信することにより、顧客情報変換サーバ３０に決済処理を実行させ、その決済処理の結果（決済結果）を顧客情報変換サーバ３０から取得して、利用者側端末１０に転送してくることから、続くＳ３００では、この決済結果を受信し、表示装置に表示する。尚、この決済結果の表示の際には、使用者に対して、インターネット２への接続を継続するか、遮断するかの指令を促す選択キーも表示する。

そして、続くＳ３１０では、決済結果を表示した結果、使用者がイン

ターネット２への接続の継続を指令したか、或いは、遮断を指令したかを判定し、接続の継続が指令された場合には、再度Ｓ２５０に移行し、逆に、接続の遮断が指令された場合には、Ｓ３２０にて、インターネット２への接続を遮断した後、Ｓ１１０に移行する。

次に、図３は、認証サーバ４にて実行される制御処理を表すフローチャートである。

図３に示すように、認証サーバ４では、まずＳ４１０（Ｓはステップを表す）にて、インターネット２を介して利用者側端末１０が接続されたか否か（換言すれば利用者側端末１０から接続要求があったか否か）を判断することにより、利用者側端末１０から接続要求が入力されるのを待つ。そして、利用者側端末１０から接続要求があると、Ｓ４２０にて、利用者側端末１０に接続要求を受信した旨を表す情報を送信し、その後、利用者側端末１０が送信してくる認証ＩＤを受信する、認証ＩＤの受付処理を実行する。

また、こうして認証ＩＤを受け付けると、今度は、Ｓ４３０に移行して、この認証ＩＤが、認証サーバ４に予め登録されている利用者の者であるか否かを判定する、認証ＩＤ判定処理を実行し、続くＳ４４０にて、その判定結果（認証結果）を、利用者側端末１０に送信する。また続くＳ４５０では、Ｓ４３０の判定処理により、利用者を認証できたか否かを判断し、認証できなければ、再度Ｓ４１０に移行し、認証できた場合には、Ｓ４６０に移行する。

Ｓ４６０では、今回認証した利用者側端末１０に装着されているＩＣカード１２内の認証データを更新する必要があるか否かを判定する。そして、認証データの更新が不要であれば、Ｓ５００にて、今回認証した利用者側端末１０に専用ＷＷＷサーバ６への接続情報を送信することにより、利用者側端末１０から専用ＷＷＷサーバ６へのアクセスを許可し

て、利用者側端末１０を専用ＷＷＷサーバ６に接続させ、再度Ｓ４１０に移行する。

また、Ｓ４６０にて、ＩＣカード１２内の認証データの更新が必要であると判断された場合には、Ｓ４７０に移行して、そのＩＣカード１２の認証データ書込ロックを解除するための情報を送信し、続くＳ４８０にて、利用者側端末１０に対して認証データの更新処理を実行させ、その更新処理により更新された認証データを認証サーバ４内の記憶装置に書き込む、といった手順で認証サーバ４側の認証データ更新処理を実行する。そして、この認証データ更新処理が終了すると、Ｓ４９０にて、認証データ書込を再ロックさせるための情報を利用者側端末１０に送信した後、Ｓ５００に移行する。

次に、図４は、専用ＷＷＷサーバ６にて実行される制御処理を表すフローチャートである。尚、専用ＷＷＷサーバ６は、認証サーバ４により接続許可された利用者側端末１０からの要求に従い、利用者側端末１０との間でインターネットショッピング等のための通信を行う通常処理を実行するが、こうした通常処理は一般的なものであるため説明を省略し、以下の説明では、本発明に係わる主要な処理についてのみ説明する。

この制御処理は、通常処理とは別に実行される処理であり、図４に示すように、処理が開始されると、まず、Ｓ５３０にて、通常処理で利用者側端末１０と通信を行った結果、利用者が利用者側端末１０を介して商品の購入決定を表す情報を送信してきたか否か、換言すれば、その商品の購入に伴う決済が必要であるか否か、を判定する。

そして、決済が必要でなければ、当該制御処理をそのまま一旦終了し、逆に、決済が必要であれば、Ｓ５４０に移行して、購入決定を送信してきた利用者側端末１０に対して、決済ＩＤを要求する。すると、利用者側端末１０は、ＩＣカード１２から決済ＩＤを読み取り、この決済ＩＤ

と利用者が入力した決済用のパスワードとを当該専用ＷＷＷサーバ６に送信してくるので、続くＳ５５０では、これら各情報を受信し、続くＳ５６０にて、その受信データと、利用者が購入を決めた商品の種別や購入代金等を表す決済用の料金情報とからなる決済データを、クローズネットワーク２０内の顧客情報変換サーバ３０に送信する。

また、このように受信データと料金情報とからなる決済データを顧客情報変換サーバ３０に送信すると、顧客情報変換サーバ３０は、そのデータに基づき決済処理を実行し、決済結果を当該専用ＷＷＷサーバ６に送信してくるので、続くＳ５７０では、その決済結果を受信し、Ｓ５７５にて、受信した決済結果から、顧客情報変換サーバ３０側で決済が正常にできたか否かを判断する。

そして、決済が正常にできた場合には、Ｓ５８０にて、利用者が購入した商品を利用者に届けるための商品配送処理を実行し、逆に、顧客情報変換サーバ３０側で決済が正常にできなかった場合には、Ｓ５８５にて、利用者側端末１０から取得した認証用の情報や料金情報を破棄することにより、今回の取引を解除する。そして、Ｓ５８０又はＳ５８５の処理実行後は、Ｓ５９０に移行して、利用者側端末１０にも決済結果を送信し、当該処理を一旦終了する。

次に、図５は、顧客情報変換サーバ３０にて実行される制御処理を表すフローチャートである。

図５に示すように、顧客情報変換サーバ３０では、まず、Ｓ６１０にて専用ＷＷＷサーバ６から送信されてくる決済データを受信したか否かを判断することにより、専用ＷＷＷサーバ６から決済データが送信されてくるのを待つ。

そして、決済データを受信すると、続くＳ６２０にて、その決済データから、決済ＩＤとパスワードを抽出し、Ｓ６３０にて、顧客・暗号化

情報データベース３２に格納された暗号化情報を用いて、決済ＩＤを解読する。尚、Ｓ６３０で行われる決済ＩＤの解読手順については、決済ＩＤの暗号化手順と一緒に後で詳しく説明する。

次に、Ｓ６３０にて、決済ＩＤを解読されると、今度は、Ｓ６４０にて、解読した決済ＩＤとパスワードとを用いて、顧客・暗号化情報データベース３２を検索することにより、決済ＩＤとパスワードとが共に一致する顧客情報（口座番号・クレジットカード番号等）を抽出する。つまり、顧客・暗号化情報データベース３２には、決済ＩＤとパスワードとに関連づけて、当該システムを利用可能な利用者の顧客情報が記憶されており、Ｓ６４０では、そのデータベースを検索することにより、解読した決済ＩＤとパスワードとに対応する顧客情報を抽出するのである。

そして、続くＳ６５０では、Ｓ６４０で抽出した顧客情報と、顧客管理システム４０側の信用調査用データベースとを使って、利用者の信用調査を行い、続くＳ６７０に移行する。尚、Ｓ６３０にて、決済ＩＤを解読できない場合や、Ｓ６４０にて、解読後の決済ＩＤとパスワードとが一致する顧客情報を抽出できない場合には、その後の処理を実行することなく、Ｓ６７０に移行する。

そして、Ｓ６７０では、Ｓ６３０～Ｓ６５０の処理の結果から、利用者は、購入代金の支払い能力を有する者であるか否か（換言すれば決済可能であるか）を判定する。そして、決済可能であれば、Ｓ６４０にて抽出した顧客情報と料金情報とを顧客管理システム４０に送信することにより、利用者の口座から購入代金を引き落とす決済処理を行い、Ｓ６９０に移行し、逆に、Ｓ６７０にて、決済できないと判断された際には、そのままＳ６９０に移行する。そして、Ｓ６９０では、決済結果を専用ＷＷＷサーバ６に送信し、当該処理を一旦終了する。

次に、ＩＣカード１２に記憶される決済ＩＤの暗号化手順、及び、顧

客情報変換サーバ３０にて暗号化された決済ＩＤから元の決済ＩＤを解読する際の暗号解読手順について説明する。

尚、ＩＣカード１２は、クローズネットワーク２０内の運用管理端末２６等を使って作成され、システム加入者に配布される。このため、顧客・暗号化情報データベース３２に格納された暗号化情報は、顧客情報変換サーバ３０で暗号化された決済ＩＤを解読するのに用いられるだけでなく、運用管理端末２６等を使って決済ＩＤを暗号化してＩＣカード１２に書き込むのにも使用される。

まず、決済ＩＤの暗号化及び暗号解読を行うために用いられる暗号化用の鍵として、本実施例では、図６Ａに示す登録語句置換シートと、図６Ｂに示す乱数シートとの２種類のデータシートが使用され、これら各データシートは、顧客・暗号化情報データベース３２に格納されている。

登録語句置換シートは、図６Ａに示すように、決済ＩＤを構成するのに使用される平仮名やローマ字等の文字と、利用者の所在地である県名を表す単語とを、１０行×１６列の表に配置し、各行に付与した０から９迄の数値と、各列に付与した００から１５迄の数値との組み合わせにより、文字又は単語を十進数表記で３桁の数値に変換できるようにしたものである。

つまり、例えば、図に示した本実施例の登録語句置換シートによれば、決済ＩＤを構成する県名が「北海道」であれば「００１」となり、決済ＩＤを構成する文字が「て」であれば「２０３」となる。

そして、この登録語句置換シートは、例えば、月単位或いは週単位というように所定期間毎に更新され、決済ＩＤを暗号化する際には、最新の登録語句置換シートが使用される。このため、顧客・暗号化情報データベース３２には、暗号化に使用する登録語句置換シートが更新される度に、その登録語句置換シートが使用期間を表す情報と一緒に追加登録

される。

つまり、顧客・暗号化情報データベース３２には、決済ＩＤの暗号化に使用した全ての登録語句置換シートが蓄積されているのである。そして、顧客情報変換サーバ３０は、暗号化された決済ＩＤを解読する際には、その決済ＩＤの作成日から暗号化に使用した登録語句置換シートを割り出し、その登録語句置換シートを用いて、決済ＩＤを解読する。

一方、乱数シートは、図６Ｂに示すように、３桁の乱数を、００から１５迄、合計１６個、順に配置することにより作成されている。この乱数シートは、予め複数作成されており、その先頭には、暗号化に使った乱数シートを特定できるようにするために、乱数シートの種別を表す識別符が付与されている。

そして、決済ＩＤの暗号化に用いる乱数シートは、登録語句置換シートと同様、月単位或いは週単位というように所定期間毎に変更される。このため、暗号化された決済ＩＤには、暗号化に使用した乱数シートを特定するために識別符が付与され、顧客情報変換サーバ３０が決済ＩＤを解読する際には、決済ＩＤに付与された識別符から暗号化に使用した乱数シートを割り出し、その乱数シートを用いて、決済ＩＤを解読する。

次に、このように構成された２つの暗号化鍵（登録語句置換シート及び乱数シート）を用いて、運用管理端末２６が実際に決済ＩＤを暗号化する手順を、図７Ａに示すフローチャートに沿って説明する。

図７Ａに示すように、運用管理端末２６が決済ＩＤを暗号化する際には、まず、Ｓ７１０にて、暗号化すべき決済ＩＤを取り込む決済ＩＤ入力処理を実行し、続くＳ７２０にて、顧客情報変換サーバ３０を介して、顧客・暗号化情報データベースから、現在暗号化用として設定されている登録語句置換シートを読み込む。そして、続くＳ７３０では、暗号化前の決済ＩＤを構成する文字列を、登録語句置換シートに記述されてい

る県名や文字の語句データに区分し、各語句データ毎に、登録語句置換シートを用いて、３桁の数値からなる語句データに変換する。

例えば、決済ＩＤが利用者を表す「和歌山なかお」という文字列であれば、決済ＩＤは、「和歌山」、「な」、「か」、「お」という４つの語句データに区分され、図６Ｃに示すように、これら各語句データは、夫々、３桁の数値「１０３」,「０１５」、「１０２」、「０００」に変換されることになる。

次に、Ｓ７３０にて、決済ＩＤが３桁の数値からなる複数の語句データに変換されると、今度は、続くＳ７４０にて、顧客情報変換サーバ３０を介して、顧客・暗号化情報データベースから、現在暗号化用として設定されている乱数シートを読み込む。

そして、続くＳ７５０では、変換後の３桁の数値からなる語句データと、乱数シートを構成する３桁の乱数とを、決済ＩＤ及び乱数シートの先頭から順に対応付け、乱数及び語句データを構成する各桁毎に、乱数から語句データを減じる演算処理を実行することにより、各語句データを乱数を用いて登録用のＩＤデータに変換する。

つまり、例えば、図６Ｃに示すように、決済ＩＤの先頭の語句データが「１０３」で、乱数シートの先頭の乱数が「２３２」である場合には、これら各データを構成する各桁の数値毎に、乱数シートから語句データを減じる方向に減算することで、「１３９」というＩＤデータを作成する。尚、減算時に乱数の数値が語句データの数値よりも小さいときには、乱数の数値に１０を加えた値から語句データの数値を減じる。

そして、このように、各語句データが、乱数シートを用いて、ＩＣカード１２への登録用のＩＤデータに変換されると、Ｓ７６０にて、各ＩＤデータを、元の決済ＩＤの語句データの並びに対応して配置し、その先頭に、暗号化に使用した乱数シートの識別符を付与することにより、

暗号化された決済ＩＤを完成させる。尚、この決済ＩＤを実際にＩＣカード１２に登録する際には、決済ＩＤを暗号化した日付も登録され、この日付情報も決済ＩＤの構成要素として取り扱われる。

一方、このように暗号化された決済ＩＤを、顧客情報変換サーバ３０にて解読する際には、図７Ｂに示す手順で、決済ＩＤが解読される。

即ち、図７Ｂに示すように、顧客情報変換サーバ３０が専用ＷＷＷサーバ６を介して利用者側端末１０から取得した決済ＩＤを暗号化する処理（Ｓ６３０）を実行する際には、まず、Ｓ８１０にて、取得した決済ＩＤの先頭に付与されている識別符を読み取り、これと同じ識別符が付与されている乱数シートを顧客・暗号化情報データベース３２から読み込む。

そして、続くＳ８２０では、その読み込んだ乱数シートを構成する各桁の数値と決済ＩＤを構成する各桁の数値とを先頭から順に対応付け、各桁の数値毎に、乱数シートから決済ＩＤを減じる演算処理を実行する。この結果、図６Ｄに示すように、決済ＩＤを構成する先頭から３桁毎の数値データ（つまりＩＤデータ）は、乱数シートを用いて、暗号化前の語句データに変換されることになる。

こうして暗号化された決済ＩＤが語句データに変換されると、今度は、Ｓ８３０にて、今回取得した決済ＩＤの作成日から、決済ＩＤの暗号化に使用した登録語句置換シートを特定し、これを、顧客・暗号化情報データベース３２から読み込む。

そして最後に、Ｓ８４０にて、その登録語句置換シートを用いて、３桁の数値空なる各語句データを、変換前の県名又は文字に変換し、これを先頭から順に配置することにより、暗号化前の決済ＩＤを復元する。この結果、図６Ｃに示すように、「和歌山なかお」という決済ＩＤが、暗号化の結果、「AS424139443859756」という決済ＩＤに変換されていても、

図６Ｄに示すように、顧客情報変換サーバ３０での暗号解読処理により、暗号化前の元の決済ＩＤが正常に復元されることになる。

以上詳述したように、本実施例の電子決済システムにおいては、利用者が、利用者側端末１０に自己のＩＣカード１２を装着し、ＩＣカード１２を使用するためのパスワードを入力すれば、利用者側端末１０が自動的に専用ＷＷＷサーバ６に接続される。このため、利用者は、極めて簡単にインターネットショッピングを楽しむことができる。また、インターネットショッピングで、実際に商品を購入する際には、その旨の意志表示（購入決定入力）を行い、表示画面上での案内に従い決済用のパスワードを入力するだけでよい。従って、本実施例の電子決済システムによれば、使用者は、従来のように決済用の各種情報を入力する必要がなく、使用者にとって極めて使い勝手のよいシステムとなる。

一方、本実施例において、専用ＷＷＷサーバ６にアクセスすることのできる端末は、認証サーバ４にて認証された利用者側端末１０だけであるため、サーバの管理者にとっては、専用ＷＷＷサーバ６の不正アクセスを防止して、専用ＷＷＷサーバ６の安全性を確保できる。

また、利用者が実際に商品を購入する際にインターネット２上を流れる決済用の情報は、暗号化された決済用の識別情報（決済ＩＤ）だけであり、利用者から購入代金を徴収するための口座番号やクレジットカード番号等の顧客情報がインターネット２上を流れることはないので、インターネット２上での顧客情報の漏洩を確実に防止でき、システムの信頼性を向上できる。

また、インターネット２に流される決済ＩＤの暗号化には、上述した２つの鍵（登録語句置換シートと乱数シート）が使用され、しかも、これらは、定期的に更新されることから、インターネット２上で決済ＩＤを第三者が取得したとしても、これを解読して悪用することは不可能で

ある。

よって、本実施例の電子決済システムによれば、利用者にとっても、システム管理者にとっても、極めて安全に商取引を行えるシステムを実現できることになる。

次に、本実施例の電子決済システムを利用して実際に商品や各種サービスの販売を行う通信販売システムの一例について説明する。

図８は、販売代行会社７０が、商品の販売若しくは各種サービスを行う各種販売会社７２からの委託を受けて、利用者７４との間の商取引を代行するようにした通信販売システム（ａ）を表している。

図８に示すように、この通信販売システム（ａ）では、販売代行会社７０が利用者７４との間の商取引を行うことから、要求受付手段としての専用ＷＷＷサーバ６、情報処理手段としての顧客情報変換サーバ３０及び顧客・暗号化情報データベース３２は、全て、販売代行会社７０にて管理される。

そして、販売代行会社７０において、専用ＷＷＷサーバ６が利用者７４から発注データ及び決済ＩＤを受けると、顧客情報変換サーバ３０に、その発注データに対応した料金情報や決済ＩＤを送信し、顧客情報変換サーバ３０が、決済ＩＤから利用者７４の顧客情報を復元して、その顧客情報が顧客・暗号化情報データベース３２に事前に登録されているか等を判定することにより、利用者７４から料金を徴収できるか否かを判定し、その判定結果を専用ＷＷＷサーバ６に送信する。

すると、専用ＷＷＷサーバ６側では、顧客情報変換サーバ３０からの判定結果に基づき、利用者７４から料金を徴収できるか否かを確認し、利用者７４から料金を徴収できる場合には、利用者７４からの受注データを、インターネット若しくは専用の通信線を介して、受注データに対応する販売会社７２（詳しくは販売会社側の発注データ受信サーバ）に

通知する。

この結果、販売会社７２からは、利用者７４が発注した商品若しくはサービスが、直接又は運送会社７８等を介して、利用者７４に提供されることになる。

また、顧客情報変換サーバ３０は、専用ＷＷＷサーバ６から受けた決済ＩＤ等に基づき、利用者７４から料金を徴収できると判断した場合には、顧客情報に対応した金融機関７６（信販会社や銀行等）に対して、料金徴収のための決済依頼を行う。

すると、金融機関７６側では、顧客情報変換サーバ３０から決済依頼と共に送信されてきた顧客情報や料金情報に基づき、利用者７４の口座から決済代金を徴収して、販売会社７２の口座に振り込む手続きが行われ、利用者７４から販売会社７２への料金の支払いが自動的に完了することになる。

このように、本実施例の電子決済システムを利用すれば、販売代行会社７０が、多数の販売会社７２からの委託を受けて、商品・サービスを代行販売する通信販売システム（ａ）を構築できる。

そして、この通信販売システム（ａ）においては、利用者は、自己の顧客情報を登録することにより販売代行会社７０から発行される一つの決済ＩＤ（一つのＩＣカード１２等）を用いて、販売代行会社７０が委託を受けている複数の販売会社７２から所望の商品又はサービスを購入できることになり、利用者にとって極めて便利な通信販売システムとなり得る。

また、販売会社７２は、販売業務を販売代行会社へ委託するだけで、商品販売若しくはサービスの受注を行うことができる。つまり、販売会社７２は、販売代行会社７０への手数料の支払い義務は生じるものの、インターネットを使った通信販売に必要な設備投資が不要となる。従っ

て、この通信販売システム（ａ）は、販売会社７２にとっても、販路の拡大に極めて便利な通信販売システムとなり得る。

尚、図８に示した通信販売システム（ａ）においては、販売会社７２が販売代行会社７０に委託することにより、図８に点線矢印で示すように、販売代行会社７０が、金融機関７６からの決済代金の徴収、或いは、利用者７４への商品・サービスの提供を行うようにすることもできる。

一方、図９は、販売会社７２が利用者７４との間で商取引のための通信を行い、決済代行会社８０が決済を行うようにした通信販売システム（ｂ）を表している。

図９に示すように、この通信販売システム（ｂ）では、要求受付手段としての機能を有する通信販売用のＷＷＷサーバ７が販売会社７２にて管理され、情報処理手段としての顧客情報変換サーバ３０及び顧客・暗号化情報データベース３２が決済代行会社８０にて管理される。

そして、販売会社７２においては、ＷＷＷサーバ７が利用者７４から発注データ及び決済ＩＤを受けると、決済代行会社８０側の顧客情報変換サーバ３０に、その発注データに対応した料金情報や決済ＩＤを送信することにより、利用者から料金を徴収できるか否かの判定を依頼（決済判定依頼）する。

すると、決済代行会社８０側の顧客情報変換サーバ３０は、決済ＩＤから利用者７４の顧客情報を復元して、その顧客情報が顧客・暗号化情報データベース３２に事前に登録されているか等を判定することにより、利用者７４から料金を徴収できるか否かを判定し、その判定結果（決済判定結果）を販売会社７２側のＷＷＷサーバ７に送信する。

すると、ＷＷＷサーバ７は、顧客情報変換サーバ３０からの判定結果に基づき、利用者７４から料金を徴収できるか否かを確認して、利用者７４から料金を徴収できる場合には、販売会社７２内の商品の配送部門

若しくはサービス提供部門に受注データを転送する。

この結果、販売会社７２から利用者７４には、利用者７４が発注した商品若しくはサービスが、直接又は運送会社７８等を介して提供されることになる。

また、顧客情報変換サーバ３０は、ＷＷＷサーバ７から受けた決済ＩＤ等に基づき、利用者７４から料金を徴収できると判断した場合には、顧客情報に対応した金融機関７６（信販会社や銀行等）に対して、料金徴収のための決済依頼を行う。

すると、金融機関７６側では、顧客情報変換サーバ３０から決済依頼と共に送信されてきた顧客情報や料金情報に基づき、利用者７４の口座から決済代金を徴収して、販売会社７２の口座に振り込む手続きが行われ、利用者７４から販売会社７２への料金の支払いが自動的に完了することになる。

このように、本実施例の電子決済システムを利用すれば、販売会社７０が利用者との間の商取引を直接行い、商取引の結果生じた料金徴収（決済）のための処理だけを決済代行会社８０が行う通信販売システム（ｂ）を構築することもできる。

そして、この通信販売システム（ｂ）においては、利用者は、自己の顧客情報を登録することにより決済代行会社８０から発行される一つの決済ＩＤを用いて、その決済代行会社８０に決済を依頼している複数の販売会社７２から所望の商品又はサービスを購入できることになり、図８に示した通信販売システム（ｂ）と同様、利用者に採って極めて便利な通信販売システムとなり得る。

また、この通信販売システム（ｂ）において、販売会社７２は、決済に必要な利用者７４の顧客情報を管理する必要がないので、システムの運用を容易に行うことができ、しかも、利用者７４は、顧客情報を販売

会社７２に知られることがないので、当該通信販売システムを安心して利用できる。

尚、図９に示した通信販売システム（ｂ）において、決済代行会社８０側の顧客情報変換サーバ３０は、必ずしも金融機関７６に対して直接決済依頼を行うようにする必要はなく、金融機関７６との間で設定した第三者が解読不能な顧客情報を販売会社７２側に転送し、図９に点線矢印で示すように、販売会社７２が金融機関７６に対して決済依頼を行うようにしてもよい。

以上本発明の一実施例について説明したが、本発明は上記実施例に限定されるものではなく、種々の態様を採ることができる。

例えば、上記実施例では、認証サーバ４及び専用ＷＷＷサーバ６は、各々別体で構成されて、インターネット２上の任意の位置に配置されるものとして説明したが、認証サーバ４としての機能（換言すれば認証手段としての機能）は、要求受付手段としての専用ＷＷＷサーバ６に組み込むようにしてもよい。

また、例えば、上記実施例では、要求受付手段としての専用ＷＷＷサーバ６と金融機関側のクローズネットワーク２０とは、インターネット２を介して接続されるものとして説明したが、これらの間は、電話回線等、専用の通信回線を介して接続するようにしてもよい。

一方、上記実施例では、ＩＣカード１２の不正使用を防止するために、ＩＣカード１２にパスワードを登録しておき、ＩＣカード１２がＩＣカードリーダ／ライタに装着された状態で利用者側端末１０がインターネット２に接続する際には、利用者にパスワードを入力させて、そのパスワードがＩＣカード１２に登録されたものと一致するか否かを判定するものとして説明したが、ＩＣカード１２の不正使用を防止するには、必ずしもパスワードを利用する必要はなく、例えば、利用者の指紋情報を

利用するようにしてもよい。また、上記実施例では、利用者が利用者側端末１０を操作する際には、キーボードやマウスを使用するものとして説明したが、こうした入力装置の一つとして、端末本体に光若しくは電波によって操作用の指令信号を送信するように構成されたリモコン装置を使用できるようにしてもよい。

そこで、次に、リモコン装置を用いて操作でき、しかも、ＩＣカード１２の不正使用を防止するために、パスワードではなく、利用者の指紋情報を用いるようにした利用者側端末１０について説明する。

図１０に示すように、この利用者側端末１０は、端末本体５０と、リモコン装置５２とから構成される。そして、端末本体５０には、ＩＣカード１２から各種情報を読み込み、必要に応じて情報を書き込むためのＩＣカードリーダ／ライタ５０ａ、インターネット接続用の通信装置５０ｂ、及び制御処理実行用のＣＰＵ，ＲＯＭ，ＲＡＭ等からなる制御部５０ｃに加えて、リモコン装置５２から光又は電波を変調することにより送信されてきた送信信号を受信するためのリモコン受信部５０ｄが設けられている。尚、これらの内、ＩＣカードリーダ／ライタ５０ａ、通信装置５０ｂ、及び制御部５０ｃは、前記実施例の利用者側端末１０にも設けられるものである。

一方、リモコン装置５２には、利用者が各種指令を入力するための操作部５２ａ、操作部を介して入力された指令信号にて光又は電波（搬送波）を変調し、変調後の信号を端末本体５０のリモコン受信部５０ｄに送信するためのリモコン送信部５２ｂが備えられると共に、利用者の指紋を取り込むための指紋センサ５２ｃが備えられている。尚、この指紋センサ５２ｃは、利用者の指紋を２次元の画像情報として取り込むためのものであり、従来より知られている光学式、感圧式、若しくは感熱式の指紋センサを利用することができる。

そして、このように構成された利用者側端末１０の制御部５０ｃにおいては、ＩＣカードリーダ／ライタ５０ａにＩＣカード１２が装着され直後、若しくは、ＩＣカードリーダ／ライタ５０ａにＩＣカード１２が装着された状態で利用者がリモコン装置５２を操作してインターネット２への接続指令を入力した場合等、端末本体５０を通信装置５０ｂを介してインターネット２に接続する際には、図１１に示すカード利用者識別処理を実行し、リモコン装置５２側では、この処理に連動して利用者から入力される指令に従い、指紋画像送信処理が実行される。

以下、このカード利用者識別処理、及び指紋画像送信処理について説明する。尚、図１０に示す利用者側端末１０を使用する際には、前述したアクセス情報，認証ＩＤ，決済ＩＤに加えて、利用者の指紋情報（利用者の指紋画像を画像処理することにより生成した指紋の特徴パラメータ）が予め記憶されたＩＣカード１２が使用される。

図１１に示すように、端末本体５０の制御部５０ｃで実行されるカード利用者識別処理では、まず利用者の指紋画像を取り込むために、端末本体５０に設けられた図示しない表示装置に、利用者に対して指紋入力を促す指紋入力要求画面を表示する（Ｓ９１０）。

すると、利用者は、リモコン装置５２の指紋センサ５２ｃに、予め指紋登録してある指を乗せ、他の指を使って操作部５２ａを操作することにより、指紋の読み取り指令を入力するので、リモコン装置５２側では、リモコン送信部５２ｂが指紋センサ５２ｃから利用者の指紋画像を取り込み（Ｓ９１５）、その取り込んだ画像データを送信用のシリアルデータに変換して送信用の信号（光又は搬送波）を変調することにより、その指紋画像を送信する（Ｓ９２０）、といった手順で、指紋画像送信処理を実行する。

このため、端末本体５０の制御部５０ｃは、上記のように表示装置に

指紋入力要求画面を表示した後は、Ｓ９３０にて、リモコン装置５２からリモコン受信部５０ｄに送信されてくる指紋画像を受信する受信処理を実行し、この処理で指紋画像が受信されると、続くＳ９４０にて、受信した指紋画像を画像処理することにより、利用者の指紋の特徴パラメータを抽出する。そして、続くＳ９５０では、ＩＣカード１２から予め登録されている指紋情報（特徴パラメータ）を読み込み、Ｓ９６０にて、この指紋情報と、Ｓ９４０で抽出した指紋の特徴パラメータとの一致度を演算する。

またこのように指紋情報の一致度が算出されると、今度は、続くＳ９７０に移行して、その一致度は、予め設定された判定値よりも大きいか否かを判断し、一致度が判定値よりも大きければ、現在リモコン装置５２を操作している利用者は、ＩＣカード１２の所有者であると判定して、インターネット２への接続を許可し（Ｓ９８０）、逆に、一致度が判定値以下であれば、現在リモコン装置５２を操作している利用者は、ＩＣカード１２の所有者ではないと判定して、不正使用防止のために、インターネット２への接続を禁止する（Ｓ９９０）。

このように、図１０に示した利用者側端末１０では、指紋情報を使って利用者がＩＣカード１２に指紋を登録したものであるか否かを判定する。このため、パスワードを使って使用者を特定する場合と同様、ＩＣカード１２の不正使用を防止できるだけでなく、その不正使用をより確実に防止することができる。また、利用者は、リモコン装置５２を使って利用者側端末１０に各種指令を入力することができるので、利用者側端末１０に接続されたキーボードやマウスを使って指令を入力する場合に比べて、操作性を向上できる。

［第２実施例］

ところで、上記実施例（第１実施例）の電子決済システムでは、顧客

情報変換サーバ３０が、銀行，クレジットカード会社等の金融機関の顧客管理システム４０に直接接続され、顧客情報変換サーバ３０が金融機関に直接決済依頼を行うことにより、料金を徴収するものとして説明したが、例えば、外部の料金徴収システムを利用して、料金を徴収するようにしてもよい。

つまり、例えば、近年では、銀行のキャッシュカードを用いて直接商品を購入できるようにしたデビットカードシステムが実用化されており、このシステムでは、システムに加入している店舗等からデビットカードによる決済依頼を受けると、そのカードに対応した金融機関の口座から購入代金を引き落として、店舗の口座に振り込むデビットカード決済センターが用いられている。そこで、顧客変換サーバとデビットカード決済センターとを専用線で結び、料金をデビットカード決済センターを介して徴収するようにしてもよい。また、この場合、利用者が料金を支払う際に、クレジットカードを用いるかデビットカード（キャッシュカード）を用いるかを選択できるようにするとよい。

そこで、次に、本発明の第２実施例として、利用者が料金の支払いにデビットカードを指定した際に、デビットカード決済センターを介して料金を徴収できるようにした電子決済システムについて説明する。

図１２は、このシステムの全体の構成を表すブロック図であり、図１３は、このシステムを構成する各サーバにおいて、利用者がデビットカードを利用する際に実行される決済用処理手順を表すフローチャートである。

図１２に示すように、第２実施例の電子決済システムは、図示しないルータやファイアウォールを介してインターネット２に接続されたクローズネットワーク２０内に、専用ＷＷＷサーバ６、顧客情報変換サーバ３０、顧客・暗号化情報データベース３２を設け、更に、外部のデビッ

トカード決済センター９０との間で専用線を介して決済用のデータを送受信するための顧客情報送信用テーブル格納サーバ６０を設けることにより構成されている。

一方、利用者側端末１０は、図１に示したものと同じであるが、デビットカード決済を利用可能なＩＣカード１２には、上述したアクセス情報、認証ＩＤ、決済ＩＤに加えて、デビットカード決済用のＩＤも記憶されており、利用者側端末１０は、利用者がデビットカードによる決済を希望すると、ＩＣカード１２からデビットカード決済用ＩＤを読み出し、クローズネットワーク２０側に送信するようになっている。

即ち、この電子決済システムにおいて、利用者側端末１０と専用ＷＷＷサーバ６との間の通信により利用者が所望の買い物を決定すると、利用者側端末１０は、利用者からデビットカード決済用の暗唱番号を受け付け、これを専用ＷＷＷサーバ６に送信する（図１２に示す①参照）。すると、専用ＷＷＷサーバ６は、利用者側端末１０に対して、デビットカード決済用ＩＤを要求し（図１２に示す②参照）、利用者側端末１０は、この要求に従い、ＩＣカード１２からデビットカード決済用ＩＤを読み出し、専用ＷＷＷサーバ６に送信する（図１２に示す③参照）。

尚、こうした利用者側端末１０と専用ＷＷＷサーバ６との間の通信（図１２に示す①，②，③）は、インターネット２を介して行われるが、これらの通信には、上述した実施例と同様、全て暗号化したデータが使用される。

また、上述のデビットカード決済用ＩＤは、デビットカードによる決済を行うために設定されるものであるが、この決済のために必ずしもデビットカード決済用ＩＤを用いる必要はなく、通常の決済ＩＤをそのまま利用するようにしてもよい。

次に、専用ＷＷＷサーバ６は、利用者側端末１０から取得したデビッ

トカード決済用の暗唱番号とＩＤとを、顧客情報変換サーバ３０に転送する（図１２に示す④参照）。すると、顧客情報変換サーバ３０側では、これら暗唱番号とＩＤとを用いて、顧客・暗号化情報データベース３２を検索することにより、顧客・暗号化情報データベース３２からデビットカード決済に必要な暗号化された顧客情報（暗号化された名前、口座番号、暗唱番号等）を抽出する（図１２に示す⑤参照）。

そして、顧客情報変換サーバ３０は、この抽出した顧客情報を解読して暗号化されていない顧客情報に戻し、この顧客情報と利用者から徴収すべき料金等を表す買い物情報とを、顧客情報送信用テーブル格納サーバ６０に転送する（図１２に示す⑥参照）。

すると、顧客情報送信用テーブル格納サーバ６０は、顧客情報変換サーバ３０からデビットカード決済用の顧客情報と買い物情報とを受けると、これを一旦送信用テーブルに格納し、その後、デビットカード決済センター９０に送信する（図１２に示す⑦参照）。

尚、顧客情報送信用テーブル格納サーバ６０は、顧客情報変換サーバ３０とデビットカード決済センター９０とが直接データ通信を行えないようにするため（具体的には、顧客・暗号化情報データベース３２内データのデビットカード決済センター９０側への漏洩防止等のため）に設けられたものであるが、このサーバ６０については、省略することもできる。

次に、デビットカード決済センター９０に顧客情報と買い物情報とが送信されると、デビットカード決済センター９０では、利用者から徴収すべき料金を利用者の銀行口座から引き落として、クローズネットワーク２０を管理している会社の口座に振り込む決済処理を行い、その決済結果を顧客情報送信用テーブル格納サーバ６０に送信してくる（図１２に示す⑧参照）。

このため、顧客情報送信用テーブル格納サーバ６０は、その決済結果を顧客情報変換サーバ３０側に転送し（図１２に示す⑨参照）、顧客情報変換サーバ３０は、その決済結果を、専用ＷＷＷサーバ６を介して、利用者側端末１０に送信することで、利用者側端末１０に決済結果を表示させる。尚、こうした決済結果の通知は、電子メールで行うようにしてもよい。

次に、上記のようにデビットカードを用いた決済を行うために利用者側端末１０、専用ＷＷＷサーバ６、顧客情報変換サーバ３０、顧客情報送信用テーブル格納サーバ６０にて実行される処理について、図１３を用いて説明する。

図１３に示す如く、利用者側端末１０では、ＩＣカードリーダ／ライタにＩＣカード１２が装着されると、端末側処理を開始し、Ｓ１０１０にて、表示装置にパスワードの入力画面を表示して、利用者からのパスワードの入力を受け付ける、パスワード受付処理を実行する。そして、利用者がパスワードを入力すると、Ｓ１０２０にて、その入力されたパスワードは、ＩＣカード１２に予め登録（記憶）されているパスワードと一致するか否かを判定し、パスワードが一致しなければ、パスワードが誤入力されたと判断して、Ｓ１０３０に移行し、上述したＳ１５０と同様の誤入力達続回数判定処理を実行し、再度Ｓ１０１０に移行する。

一方、Ｓ１０２０にて、利用者が入力したパスワードとＩＣカード１２に登録されたパスワードとが一致していると判断されると、Ｓ１０４０に移行し、ＩＣカード１２からインターネット２上の専用ＷＷＷサーバ６へのアクセス情報を読み込み、その読み込んだアクセス情報に従い、利用者側端末１０を、図示しないＩＳＰを介して、インターネット２上の専用ＷＷＷサーバ６に接続させる。

尚、本実施例では、図１に示したシステムのように認証サーバ４が設

けられていないので、ＩＣカード１２の個人認証が完了すると、利用者側端末１０は、直接、専用ＷＷＷサーバ６に接続されることになるが、図１に示したシステムのように認証サーバ４を設け、この認証サーバ４にて個人認証を行った後、利用者側端末１０を、専用ＷＷＷサーバ６に接続するようにしてもよい。

こうして、利用者側端末１０が専用ＷＷＷサーバ６に接続されると、今度は、Ｓ１０５０に移行して、上述したＳ２５０と同様のインターネットアクセス処理を実行する。また、このアクセス処理実行時には、周期的にＳ１０６０の処理を実行することにより、専用ＷＷＷサーバ６から決済方法の要求があったか否かを判断する。

つまり、専用ＷＷＷサーバ６側では、上記のように利用者側端末１０からアクセスされると、利用者側端末１０からの要求に従い、利用者側端末１０に対して各種ページ（ホームページ）を提供する、ＷＷＷサーバとしての処理（Ｓ１２１０）を実行するが、この処理の間は、利用者側端末１０から商品の購入指令が入力されて、料金徴収のための決済が必要になったか否かを判断し（Ｓ１２２０）、決済が必要になると、利用者側端末１０に対して、決済方法の選択画面を送信することにより、決済をクレジットカードで行うか、デビットカードで行うかを利用者に選択させる、決済方法要求処理を実行する（Ｓ１２３０）。

このため、利用者側端末１０では、Ｓ１０６０にて、専用ＷＷＷサーバ６から決済方法の要求があったか否かを判断し、決済方法の要求があった場合には、Ｓ１０７０に移行して、専用ＷＷＷサーバ６から送信されてきた決済方法の選択画面を表示装置に表示し、その表示画面上で利用者が決済方法を入力するのを受け付け、利用者が選択した決済方法を専用ＷＷＷサーバ６に送信する、決済方法受付・送信処理を実行する。

こうして、利用者側端末１０から専用ＷＷＷサーバ６に決済方法が送

信されると、専用ＷＷＷサーバ６側では、利用者が選択した決済方法は、デビットカードによるものか、或いは、クレジットカード等の他のカードによるものかを判断する（Ｓ１２４０）。そして、利用者がデビットカードによる決済を要求している場合には、専用ＷＷＷサーバ６は、利用者側端末１０に対して、デビットカードによる決済確認用の暗唱番号を要求し（Ｓ１２５０）、その後は、利用者側端末１０から送信されてくる暗唱番号等のデータを受信して、顧客情報変換サーバ３０に送信し、顧客情報変換サーバ３０から送信されてきたデータを受信して、利用者側端末１０に送信する、所謂中継処理を実行する（Ｓ１２６０）。

尚、専用ＷＷＷサーバ６側の処理において、Ｓ１２４０にて、利用者が選択した決済方法は、デビットカードではなく、他のカード（クレジットカード等）によるものであると判断された場合には、図１に示したシステムにおける決済用の処理と同様に、そのカードに対応した決済用処理を行い、利用者側端末１０や顧客情報変換サーバ３０も、この専用ＷＷＷサーバ６側の処理に対応した決済用の処理を行う。つまり、利用者がデビットカードを用いた決済を要求していなければ、図１に示したシステムと同様の決済手順で、金融機関から料金を直接徴収するための処理を行う。

次に、利用者側端末１０では、Ｓ１０７０にて利用者から決済方法を受け付けて専用ＷＷＷサーバ６に送信すると、専用ＷＷＷサーバ６から決済確認用の暗唱番号が要求されるため、続くＳ１０８０では、この要求に従い、暗唱番号の入力画面を表示装置に表示し、利用者に対して、デビットカードによる決済確認用の暗証番号の入力を促す。そして、利用者から決済確認用の暗唱番号が入力されると、これを暗号化して専用ＷＷＷサーバ６に送信する。すると、専用ＷＷＷサーバ６は、上述した中継処理により、この暗証番号を顧客情報変換サーバ３０に送信する。

このように、利用者側端末１０から送信された決済確認用の暗唱番号が専用ＷＷＷサーバ６を介して顧客情報変換サーバ３０に入力されると、顧客情報変換サーバ３０側では、デビットカード決済用の処理を実行する。

そして、この処理では、まずＳ１３１０にて、専用ＷＷＷサーバ６から入力された決済確認用の暗唱番号を解読し、決済対象となっている利用者が当該電子決済システムに予め登録された利用者であるか否かを判定する所謂認証処理を行い、Ｓ１３２０にて、Ｓ１３１０の処理の結果、暗証番号から利用者を認証できたか否かを判断する。

そして、Ｓ１３２０にて、利用者を認証できなければ、Ｓ１３７０に移行して、決済結果（この場合、決済不能を表す情報）を、専用ＷＷＷサーバ３０を介して利用者側端末１０に送信し、逆にＳ１３２０にて、利用者を認証できた場合には、Ｓ１３３０に移行して、利用者側端末１０に対してデビットカード決済用ＩＤを要求する。尚、この要求は、専用ＷＷＷサーバ３０を介して行われる。

このため、利用者側端末１０では、Ｓ１０８０にて、決済確認用暗唱番号を送信した後は、続くＳ１０９０にて、顧客情報変換サーバ３０からのデビットカード決済用ＩＤの要求を受け付け、この要求に従い、ＩＣカード１２からデビットカード決済用ＩＤを抽出し、これを暗号化して、専用ＷＷＷサーバ６に送信する。尚、顧客情報変換サーバ３０から専用ＷＷＷサーバ６を介して決済不能を表す決済結果が送信されてきた場合、利用者側端末１０は、Ｓ１０９０の処理を実行することなく、Ｓ１１００に移行し、その決済結果（決済不能）を表示装置に表示する。

尚、既述したように、デビットカード決済時に、通常の決済ＩＤを使用するようにしたシステムであれば、Ｓ１３３０の処理では、その決済ＩＤを要求し、Ｓ１０９０の処理では、ＩＣカード１２から決済ＩＤを

読み出し、これを暗号化して送信することになる。

次に、利用者側端末１０から専用ＷＷＷサーバに送信されたデビットカード決済用ＩＤは、顧客情報変換サーバ３０に転送される。

このため、顧客情報変換サーバ３０では、Ｓ１３４０にて、そのデビットカード決済用ＩＤを受信して解読し、その解読した決済用ＩＤを用いて、デビットカード決済に必要な顧客情報（暗号化された名前、口座番号、暗唱番号等）を顧客・暗号化情報データベース３２から抽出する。そして、続くＳ１３５０では、その抽出した顧客情報を解読して暗号化されていない顧客情報に戻し、この顧客情報と買い物情報とを、顧客情報送信用テーブル格納サーバ６０に送信する。

すると、顧客情報送信用テーブル格納サーバ６０側では、顧客情報変換サーバ３０から送信されてきた顧客情報と買い物情報と受信して、一旦、送信用テーブルに格納し（Ｓ１４１０）、続くＳ１４２０にて、デビットカード決済センター９０の決済用コンピュータに専用線を介して接続した後、Ｓ１４３０にて、送信用テーブルに格納した顧客情報と買い物情報とを含む決済要求を、デビットカード決済センター９０の決済用コンピュータに送信する。

そして、このようにデビットカード決済センター９０に決済要求を送信すると、デビットカード決済センター９０側では、上述した決済処理が実行されて、その決済結果が、デビットカード決済センター９０から顧客情報送信用テーブル格納サーバ６０に送信されてくるので、顧客情報送信用テーブル格納サーバ６０は、Ｓ１４４０にて、その決済結果を受信して、顧客情報変換サーバ３０に送信する。

このため、顧客情報変換サーバ３０では、Ｓ１３５０にて顧客情報と買い物情報とを顧客情報送信用テーブル格納サーバ６０に送信した後は、Ｓ１３６０にて、このサーバ６０から決済結果が送信されてくるのを待

ち、Ｓ１３６０にて、その決済結果を受信すると、Ｓ１３７０に移行して、その決済結果を、専用ＷＷＷサーバ６を介して、利用者側端末１０に送信する。

また、利用者側端末１０では、Ｓ１０９０にて、デビットカード決済用ＩＤを専用ＷＷＷサーバ６に送信した後は、Ｓ１１００にて、専用ＷＷＷサーバ６から決済結果が送信されてくるのを待ち、その決済結果を受信すると、これを表示装置に表示する。

尚、上述したように、決済結果の利用者への通知を、電子メールで行うようにする場合には、顧客情報送信用テーブル格納サーバ６０におけるＳ１４４０の処理で、顧客情報変換サーバ３０に決済結果を送信するのに代えて、予め登録された利用者のメールアドレスに対して電子メールで決済結果を送信するようにするか、或いは、顧客情報変換サーバ３０におけるＳ１３７０の処理で、利用者側端末１０に決済結果を送信するのに代えて、予め登録された利用者のメールアドレスに対して電子メールで決済結果を送信するようにすればよい。

以上説明したように、本実施例の電子決済システムでは、図１に示したシステムと同様、クレジットカード等を利用した決済に加えて、外部のデビットカード決済センターを利用したデビットカードによる決済を行うことができる。このため、利用者による決済方法の選択の幅を拡大でき、利用者にとって利用しやすい販売システムを構築できる。

また、利用者側端末１０と専用ＷＷＷサーバ６との間の通信（図１２に示す①，②，③）は、インターネット２を介して行われるが、これらの通信には暗号化したデータが使用され、しかも、決済に必要な顧客情報（名前、口座番号、暗唱番号等）は、インターネット２上を流れないため、図１に示したシステムと同様、システムの信頼性を確保できる。

尚、図１３のフローチャートにおいて、顧客情報変換サーバは、Ｓ１

３１０にて利用者側端末から決済確認用の暗唱番号を取得し、この暗唱番号を用いて利用者を認証した後、デビットカード決済のための処理を実行するものとして説明したが、この暗証番号を用いた認証は、必ずしも行う必要はない。

また、上記第２実施例の決済システムでは、デビットカードによる決済を行うために、当該システムの中心となるクローズネットワーク２０内に設置されている顧客・暗号化情報データベース３２にデビットカード決済用の顧客情報を記憶しておき、デビットカード決済時には、顧客情報変換サーバ３０が、顧客・暗号化情報データベース３２から、利用者の顧客情報を読み出し、その顧客情報と買い物情報とを、顧客情報送信用テーブル格納サーバ６０を介して、デビットカード決済センター９０に送信するものとして説明したが、例えば、当該システムで利用可能なデビットカード決済用の顧客情報については、デビットカード決済センター９０側のデータベースに登録しておき（或いは、当該システム用データベースをデビットカード決済センター９０側に設置しておき）、デビットカードによる決済時には、顧客情報変換サーバ３０が、利用者側端末１０から取得したデビットカード決済用の暗唱番号とＩＤを、デビットカード決済センター９０に直接（若しくは顧客情報送信用テーブル格納サーバ６０を介して）送信するようにしてもよい。つまり、このようにしても、デビットカード決済センター９０側では、暗証番号とＩＤとに基づき顧客情報を取得して、利用者の銀行口座から利用料金を徴収することができる。

［第３実施例］

次に、上述した第１実施例及び第２実施例では、インターネット等の広域ネットワークを使って利用者から料金を徴収する電子決済システムについて説明したが、本発明の広域ネットワーク用情報処理システムに

よれば、広域ネットワークに流れる情報を第三者が取得しても、その情報から利用者個人の情報を取得するのは困難であり、極めてセキュリティ性の高いシステムを構築できることから、本発明のシステムを利用すれば、利用者の個人情報を管理する各種サービスを提供することも可能である。

例えば、上記実施例において、利用者側端末１０の本体（専用端末の他、パーソナルコンピュータ，携帯電話等の情報機器、テレビゲーム機，テレビ等の家電製品；自動車用ナビゲーション装置等の車載機器等を含む)、若しくは、これをリモート操作するためのリモコン装置に、人体用のバイタル測定器（脈拍、血圧、体脂肪、酸素、二酸化炭素等の測定器）を組み込み、その測定器による測定値をデータ化して、識別情報と一緒に、システム専用ＷＷＷサーバに暗号化(例えば 128bitSSL）送信するようにし、サーバ側では、そのデータを利用者の健康管理用データベースに蓄積し、更に、蓄積されたデータに基づき、各利用者の健康状態を定期的にチェックし、電子メールでチェック結果を送信するようにすることで、利用者の健康チェックを行うサービスを提供することができる。

つまり、このようなサービスを提供する健康管理システムを一般的なインターネットサービスとして実現すると、個人情報が漏れる虞があるため、利用者は安心してサービスを受けることができないが、上記実施例システムの認証方法及び個人情報の伝送方法を利用すれば、システムのセキュリティ性を確保することができるため、利用者は、安心して利用することができるようになり、しかも、上記システムによれば、疾病予防にも繋がることから、利用者にとって利用し易く、且つ、付加価値の高いサービスを実現できることになる。また、健康管理用データベースに蓄積した利用者個人のデータは、利用者の承諾を得て、利用者の通院時に病院に提供するようにすれば、医師による診察精度を向上させる

こともできる。

尚、この健康管理システムにおいて、健康管理用データベースに蓄積した利用者個人のデータは、電子メール等で送信する以外にも、利用者が端末操作によって、自由に確認できるようにするとよい。

また、上記健康管理システムにおいて、健康管理用データベースと、地域の病院の院内ネットワークや個人医院の診療用コンピュータとを通信回線で接続し、健康管理用データベースを、これら各医療機関が利用できるようにすれば、各医療機関が利用者個人のデータを共通の患者データとして共有することが可能になり、更に、各医療機関が、健康管理用データベースに、レセプトデータ等の診療履歴を書き込み、その診療履歴をも各医療機関で共用できるようにすれば、薬剤の二重投与防止、薬物の飲み合わせによる危険回避等にも役立つことになる。

また、上記実施例において用いるＩＣカードを、複数の医療機関共通の診察券として利用できるようにすれば、利用者は、カード１枚で複数の医療機関で診察を受けることができるようになり、利用者の利便性を向上できる。また、医療機関側では、患者毎の個人情報の共有により診察精度を向上でき、しかも、セキュリティ性の高いデータベースを利用して信頼性の高い診療を行うことができるので、医療機関にとっても非常に有益なものとなる。

そこで、次に、本発明の第３実施例として、利用者個人の健康状態や医療機関での診療履歴等を健康管理用の個人情報として蓄積するための個人情報データベースを構築し、利用者個人及び利用者から許可された医療機関側の医師がその個人情報データベースに自由にアクセスして、個人情報の更新或いは検索が行えるようにした健康管理システムについて説明する。

尚、以下の説明において、図１４は、この健康管理システムの全体の

構成を表すブロック図であり、図１５は、このシステムを構成する利用者側端末１０、専用ＷＷＷサーバ６、顧客情報変換サーバ３０において、利用者や医師が個人情報データベース６４にアクセスする際に実行される個人情報の登録・閲覧手順を表すフローチャートであり、図１６は、個人情報データベース６４を管理する個人情報管理サーバ６２において、利用者や医師からの要求に従い実行される個人情報管理処理を表すフローチャートである。

図１４に示すように、本実施例の健康管理システムは、図示しないルータやファイアウォールを介してインターネット２に接続されたクローズネットワーク２０内に、上記各実施例と略同様に機能する専用ＷＷＷサーバ６、顧客情報変換サーバ３０、及び、顧客情報変換サーバ３０及び顧客・暗号化情報データベース３２を備える。

また、クローズネットワーク２０内には、上述した個人情報データベース６４、これを管理する個人情報管理サーバ６２、個人情報データベース６４に蓄積された個人情報を利用可能な医師を表す情報が登録された医師情報データベース６６、及び、医師に対して個人情報を公開するのに用いられる医師閲覧専用ＷＷＷサーバ６８が設けられている。尚、本実施例においては、顧客情報変換サーバ３０に加えて、個人情報管理サーバ６２が、本発明の個人情報管理手段（換言すれば情報処理手段）として機能する。また、医師情報データベース６６は、本発明（請求項１１）の個人情報利用者データベースに相当する。

一方、利用者側端末１０には、利用者個人の健康状態（例えば、脈拍、血圧、体脂肪、酸素、二酸化炭素、血流、血液、髪の毛、爪、口内皮膜、口内粘膜、唾液等の少なくとも一つ）を測定するためのバイタル測定器１０ａが設けられており、このバイタル測定器１０ａにて測定されたデータは、ＩＣカード１２に記憶されたインターネット２への接続用のア

クセス情報、認証情報としての認証ＩＤ（インターネット２に認証サーバが設置されている場合)、暗号化された識別情報としての接続用暗号ＩＤ）を利用して、利用者側端末１０から専用ＷＷＷサーバ６に送信される。

即ち、この健康管理システムにおいて、個人情報の登録者である利用者が、バイタル測定器１０ａを利用して現在の健康状態を測定すると、利用者側端末１０は、その測定データに接続用暗号ＩＤを付与した更新要求を専用ＷＷＷサーバ６に送信し、同じく利用者が、利用者側端末１０に対して、個人情報の閲覧要求を入力すると、利用者側端末１０は、専用ＷＷＷサーバ６に、閲覧条件に接続用暗号ＩＤを付与した閲覧要求を送信する。

また、個人情報の閲覧又は更新が許可された医療機関側の医師が、利用者側端末１０に対して、個人情報の閲覧若しくは更新要求を入力すると、利用者側端末１０は、専用ＷＷＷサーバ６に、閲覧若しくは更新が要求された個人情報の利用者個人を表す情報に接続用暗号ＩＤを付与した要求信号を送信する。

そして、専用ＷＷＷサーバ６は、利用者側端末１０から送信されてきたこれらの情報を顧客情報変換サーバ３０に転送し、顧客情報変換サーバ３０は、接続用暗号ＩＤを解読して、利用者が顧客・暗号化情報データベース３２に登録されているか否かを判断することにより、今回要求を送信してきた利用者は、当該システムの顧客であるか否かを判断し、顧客であれば、顧客・暗号化情報データベース３２に記憶された顧客情報（本実施例では、個人情報の登録者か医師かを表す情報、個人情報の登録者であれば閲覧用情報の送信方法や送信先を表す情報、医師であれば所属病院を表す情報等）と利用者が要求してきた閲覧・更新等の内容とを、個人情報管理サーバ６２に転送する。尚、利用者側端末１０から

のデータにバイタル測定器１０ａによる測定データが含まれる場合には、このデータも個人情報管理サーバ６２に転送される。

そして、個人情報管理サーバ６２側では、個人情報の登録者である利用者が測定データを送信してきた際には、その利用者に対応した個人情報データベース６４内の個人情報を更新し、個人情報の登録者である利用者が個人情報の閲覧を要求してきた際には、個人情報データベース６４からその要求に対応した閲覧用の個人情報を抽出すると共に、顧客情報変換サーバ３０から取得した顧客情報に基づき、閲覧用個人情報の送付方法や送付先を特定して、抽出した閲覧用の個人情報を利用者に送信する。

例えば、利用者が、個人情報を専用ＷＷＷサーバ６を介して取得したいと希望していれば、専用ＷＷＷサーバ６が提供するホームページ上に匿名で個人情報を公開し、利用者が、電子メールで閲覧用の個人情報を取得したいと希望していれば、顧客情報に付与されたメールアドレスに閲覧用の個人情報を送信し、利用者が、インターネット２を利用しない通信手段（例えば、ファクシミリ、電話等）で閲覧用の個人情報を取得したいと希望していれば、その希望する通信手段を利用して、閲覧用の個人情報を利用者に送信する。

また、個人情報管理サーバ６２は、個人情報の閲覧・更新が許可された医師が個人情報の要求を送信してきた際には、個人情報データベース６４からその要求に対応した個人の個人情報を抽出して、医師の顧客情報と共に、医師閲覧専用ＷＷＷサーバ６８に転送する。すると、医師閲覧専用ＷＷＷサーバ６８は、個人情報を要求してきた医師が所属又は運営する院内ネットワークに接続し、医師が所有するコンピュータでのみ閲覧できる医師専用のホームページを開き、医師に対して特定の個人情報を提供する。

以下、このように個人情報を管理するために利用者側端末１０及びクローズネットワーク２０内の各サーバ６．３０．６２で実行される処理について図１５及び図１６を用いて説明する。

図１５に示す如く、利用者側端末１０では、ＩＣカードリーダ／ライタにＩＣカード１２が装着されると、端末側処理を開始し、表示装置にパスワードの入力画面を表示して、利用者からのパスワードの入力を受け付ける、パスワード受付処理を実行する（Ｓ２０１０）。そして、利用者がパスワードを入力すると、その入力されたパスワードは、ＩＣカード１２に予め登録されているパスワードと一致するか否かを判定し（Ｓ２０２０）、パスワードが一致しなければ、パスワードが誤入力されたと判断して、上述したＳ１５０と同様の誤入力達続回数判定処理を実行し（Ｓ２０３０）、再度Ｓ２０１０に移行する。

一方、利用者が入力したパスワードとＩＣカード１２に登録されたパスワードとが一致していると判断されると、ＩＣカード１２からインターネット２上の専用ＷＷＷサーバ６へのアクセス情報を読み込み、その読み込んだアクセス情報に従い、利用者側端末１０を、図示しないＩＳＰを介して、インターネット２上の専用ＷＷＷサーバ６に接続する（Ｓ２０４０）。

尚、インターネット２上に認証サーバ４を設けたシステムであれば、利用者側端末１０は、この認証サーバ４に認証ＩＤを送信して認証サーバ４で個人認証が行われた後、上記Ｓ２０１０移行の処理を実行することになる。

このように専用ＷＷＷサーバ６に接続されると、利用者側端末１０は、上述したＳ２５０と同様のインターネットアクセス処理を実行する（Ｓ２０５０）。そして、このインターネットアクセス処理実行時に、利用者から、バイタル測定器１０ａの操作若しくはキーボードやマウスの操作

によって、個人情報の更新又は閲覧要求が入力されると、専用ＷＷＷサーバ６に対して個人情報管理サーバへの接続要求を送信する（Ｓ２０６０）。

一方、専用ＷＷＷサーバ６側では、上記のように利用者側端末１０からアクセスされると、利用者側端末１０からの要求に従い、利用者側端末１０に対して各種ページ（ホームページ）を提供する、ＷＷＷサーバとしての処理を実行するが（Ｓ２２１０）、この処理の間は、利用者側端末１０から個人情報管理サーバへの接続要求が送信されてきたか否かを判断し（Ｓ２１２０）、接続要求が送信されてくると、接続要求を送信してきた利用者側端末１０に対して、接続用暗号ＩＤを要求する（Ｓ２１３０）。

このため、利用者側端末１０では、専用ＷＷＷサーバ６から接続用暗号ＩＤが要求されるのを待ち、接続用暗号ＩＤが要求されると、接続用暗号ＩＤに利用者からの要求内容を付与した（バイタル測定器１０ａによる測定データがある場合にはそのデータも付与した）要求信号を生成し、これを専用ＷＷＷサーバ６に送信する（Ｓ２０７０）。

すると、専用ＷＷＷサーバ６側では、この要求信号を受信し、顧客情報変換サーバ３０へと転送する（Ｓ２１４０）。このため、顧客情報変換サーバ３０側では、この転送されてきた要求信号（接続用暗号ＩＤ＋要求）を受信し（Ｓ２２１０）、その受信した接続用暗号ＩＤを解読して、顧客・暗号化情報データベース３２から、接続用暗号ＩＤに対応する顧客情報を抽出し（Ｓ２２２０）、その後、接続用暗号ＩＤに対応する顧客情報を抽出できたか否か、換言すれば、今回要求を送信してきた利用者は当該システムに登録された顧客（具体的には、個人情報の登録者又は閲覧許可された医師）であるか否かを判定し（Ｓ２２３０）、予め登録された利用者でなければ、その旨を表す処理結果を、専用ＷＷＷサーバ６

を介して、利用者側端末１０に送信する（Ｓ２２６０）。

また、顧客情報変換サーバ３０は、今回要求を送信してきた利用者が個人情報の登録者又は閲覧許可された医師であると判断すると、利用者からの要求を表す情報と、顧客・暗号化情報データベース３２から取得した顧客情報とを、個人情報管理サーバ６２に送信する（Ｓ２２４０）。

すると、個人情報管理サーバ６２側では、これらの情報に従い、個人情報データベース６４内の個人情報を更新したり個人情報データベース６４から閲覧用の個人情報を取得するための個人情報管理処理（図１６参照）を実行し、その処理結果を、顧客情報変換サーバ３０に送信してくるので、顧客情報変換サーバ３０は、個人情報管理サーバから処理結果が送信されてくるのを待ち（Ｓ２２５０）、処理結果を受信すると、その受信した処理結果を、専用ＷＷＷサーバ６に送信する（Ｓ２２６０）。

また、このように、顧客情報変換サーバ３０から専用ＷＷＷサーバ６に処理結果が転送されてくると、専用ＷＷＷサーバ６は、Ｓ２２６０にて、その処理結果を利用者側端末１０に表示可能なデータに変換して、利用者側端末１０に送信する。このため、利用者側端末１０は、接続用暗号ＩＤを付与した要求信号を送信した後（Ｓ２０７０）は、専用ＷＷＷサーバ６から処理結果が送信されてくるのを待ち、専用ＷＷＷサーバ６から処理結果が送信されてくると、これを受信して、所定の表示装置に表示させる（Ｓ２０８０）。

この結果、利用者は、今回専用ＷＷＷサーバ６に対して要求した個人情報の更新若しくは閲覧が顧客情報変換サーバ３０で受け付けられ、個人情報管理サーバ６２が、その要求に従って処理を実行したか否かを確認できる。

尚、この一連の処理で利用者側端末１０に送信される処理結果は、利用者からの要求を受け付けたか否か、要求を受け付けた場合には、要求

に従って処理を完了したか否かを表す情報だけであり、閲覧用の個人情報等については、個人情報管理サーバ６２側の処理により、利用者が予め指定した方法で、利用者側端末１０若しくは利用者側の情報端末（ファクシミリ装置・電話機・パーソナルコンピュータ等）に直接送信される。

次に、個人情報管理サーバ６２が顧客情報変換サーバ３０から受け取った要求信号（顧客情報＋要求）に従い実行する個人情報管理処理について説明する。

図１６に示すように、個人情報管理サーバ６２は、まず、Ｓ２３１０にて、顧客情報変換サーバ３０からの顧客情報を受信したか否かを判断する。そして、顧客情報を受信した場合には、Ｓ２３２０に移行して、顧客情報から、今回要求を送信してきた顧客は、個人情報データベース６４に自己の健康状態を表す個人情報を登録している利用者であるか、或いは、個人情報を登録した利用者から閲覧が許可されている医師（換言すれば、医師情報データベース６６に登録されている医師）であるかを判断する。

そして、今回要求を送信してきた顧客が、個人情報を登録している利用者であれば、Ｓ２３３０に移行して、利用者からの要求は、個人情報（つまりバイタル測定器１０ａで測定された測定データ）の更新（登録）であるか、個人情報の閲覧であるかを判断し、個人情報の登録であれば、Ｓ２３４０にて、顧客情報変換サーバ３０から受け取った顧客情報に付与されている測定データを新たなデータとして個人情報データベース６４に書き込み、Ｓ２３５０にて、その登録結果（書き込んだ内容）を、利用者への送信データに変換して、図示しないデータ送信用サーバに転送する。この結果、データ送信用サーバからは、利用者が予め指定した方法で、登録結果が送信される。

尚、データ送信用サーバからの登録結果の送信は、電子メールやファクシミリ等で行われ、利用者側端末１０に対して直接送信しないため、個人情報管理サーバ６２は、別途、登録処理が完了した旨を表す処理結果を、顧客情報変換サーバ３０に送信する（Ｓ２３６０）。

一方、Ｓ２３３０にて、今回受け取った利用者からの要求は、個人情報の閲覧要求であると判断された場合には、Ｓ２３７０に移行して、利用者からの要求に従い個人情報データベース６４を検索して、利用者から要求された閲覧用の個人情報を抽出し、続くＳ２３８０にて、その抽出した個人情報を、利用者への送信データに変換して、図示しないデータ送信用サーバに転送する。この結果、データ送信用サーバからは、利用者が予め指定した方法で、閲覧したい個人情報が送信される。

尚、上述したように、データ送信用サーバからの個人情報の送信は、電子メールやファクシミリ等で行われ、利用者側端末１０に対して直接送信しないため、個人情報管理サーバ６２は、別途、個人情報の送信処理が完了した旨を表す処理結果を、顧客情報変換サーバ３０に送信する（Ｓ２３６０）。

次に、Ｓ２３２０にて、今回顧客情報変換サーバ３０から受け取った要求は医師情報データベース６６に登録された医師からの要求であると判断された際には、Ｓ２３９０にて、医師情報データベース６６を検索することにより、医師が閲覧を許可されている個人情報を特定し、続くＳ２４００にて、その特定された閲覧可能個人情報を、個人情報データベース６４から抽出する。

そして、その後は、Ｓ２４１０にて、個人情報データベース６４から抽出した閲覧可能個人情報を、医師閲覧専用ＷＷＷサーバ６８へ転送することにより、医師閲覧専用ＷＷＷサーバ６８に対して、医師が所有するコンピュータでのみ閲覧できる医師専用のホームページを開設させ、

続くＳ２３６０にて、その旨を表す処理結果を、顧客情報変換サーバ３０に送信し、当該処理を一旦終了する。

また次に、Ｓ２３１０にて、顧客情報変換サーバ３０から顧客情報を受信していないと判断された場合には、Ｓ２４２０に移行して、医師閲覧専用ＷＷＷサーバ６８から、医師に公開していたホームページ上で、例えば、診療履歴の追加、薬剤の投与履歴の追加等がなされ、個人情報データベース６４に登録された利用者の個人情報を更新する必要があるか否かを判断する。

つまり、本実施例の医師閲覧専用ＷＷＷサーバ６８は、医師が患者の個人情報として診療履歴（換言すればカルテ情報）や薬剤の投薬履歴を書き込める形態で、医師に個人情報を公開するようにされていることから、Ｓ２４２０では、医師閲覧専用ＷＷＷサーバ６８が医師に公開したホームページ上で、医師による個人情報（診療履歴、投薬履歴等）の書き込みが合ったか否かを判断するのである。

そして、Ｓ２４２０にて、個人情報の更新が必要ないと判断されると、当該処理をそのまま終了し、逆に、個人情報の更新が必要であると判断されると、Ｓ２４３０に移行する。そして、Ｓ２４３０では、医師閲覧専用ＷＷＷサーバ６８から、更新すべき個人情報を取得し、続くＳ２４４０にて、その取得した個人情報に従い、個人情報データベース６４内の情報を書き換え、当該処理を終了する。

以上説明したように、本実施例の健康管理システムにおいては、利用者側端末１０にバイタル測定器１０ａを設け、バイタル測定器１０ａで測定した利用者の健康状態（脈拍、血圧、体脂肪、酸素、二酸化炭素、血流、血液、髪の毛、爪、口内皮膜、口内粘膜、唾液等）を表す測定データを、個人情報管理サーバ６２側に送信することで、その測定データの履歴を個人情報として、個人情報管理サーバ６２で管理し、しかも、

必要に応じて、その個人情報を、利用者本人若しくは医師が確認できるようにされている。

また、医師は、診療履歴や薬剤の投薬履歴等を、患者の個人情報として追加できるので、医師閲覧専用ＷＷＷサーバを利用して、患者の治療・診断に要するあらゆる情報を取得でき、患者にとって最適な治療・診断を行うことができる。

また、本実施例の健康管理システムを利用すれば、患者は、医師に対して、定期的に患者の健康状態をチェックして健康維持のためのアドバイスを診療履歴等に書き込んでくれるよう依頼しておくことにより、病院に行くことなく、健康状態を保つことができるようになる。

また、特に、患者である利用者が複数の医療機関の医師に対して個人情報の閲覧を許可すれば、複数の医療機関で患者個人の健康状態や診療履歴、投薬履歴等を共用することが可能となり、各医療機関で患者に対する診察・治療をより高度に行うことができるようになる。また、薬剤の二重投与の防止や、薬剤の飲み合わせによる危険回避等にも役立つ。

そして、本実施例の健康管理システムにおいては、こうした高度な医療をインターネットを介して実現できるにも関わらず、上記各実施例と同様、利用者個人の健康状態を表す個人情報が外部に漏れることはなく、また、例え、個人情報の一部が外部に漏れたとしても、その個人情報から利用者個人を特定することはできないことから、利用者は、本実施例の健康管理システムを安心して利用することができる。

尚、本実施例では、個人情報データベース６４に蓄積される利用者の個人情報を閲覧できるのは、利用者個人と医師であるものとして説明したが、クローズネットワーク２０内に、医師閲覧専用ＷＷＷサーバ６８に加えて、薬剤師閲覧専用ＷＷＷサーバを設置し、個人情報データベース６４に個人情報を登録している利用者が許可した薬剤師から、その利

用者に対する投薬履歴の閲覧要求があった際には、個人情報管理サーバ６２が、個人情報データベース６４から、薬剤師が閲覧を許可されている個人情報の内の投薬履歴のみを抽出し、これを、薬剤師閲覧専用ＷＷＷサーバを介して、薬剤師に公開するようにしてもよい。そして、このようにすれば、薬剤の二重投与等をより確実に防止できる。

また、本実施例で用いられるＩＣカード１２を、複数の医療機関共通の診察券として利用出来るようにすれば、利用者はカード１枚で複数の医療機関で診察や処置を受けることができ、利用者の利便性を向上させることができる。また、この場合、医療機関の診察室に利用者側端末１０を設置するようにすれば、医師は、診察券である患者個人のＩＣカード１２を利用して、患者の個人情報を取得できることになるので、クローズネットワーク２０に設ける医師閲覧専用ＷＷＷサーバ６８を不要にすることもできる。

［応用例］

以上、本発明の実施例として、電子決済システム及び健康管理システムについて説明したが、本発明は、上記各実施例で説明したシステムを拡大或いは変更することにより、利用者にとってより便利で安全なシステムを構築できる。

以下、そのシステムの一例を、本発明の応用例として説明する。

・応用例１…処方箋システム

上記のように、第３実施例の健康管理システムでは、薬物の二重投与の防止や、薬剤のの見合わせによる危険回避を確立する上で、家庭で使うＩＣカードを各医療機関共通の診察券として利用し、また院外処方の病院において、診察室に専用の端末（ＳＴＢ・パーソナルコンピュータ・テレビ）を設置し、患者のＩＣカードを挿入することで自動認証を行い、当該患者専用のデータベースに接続され、医療履歴データを医師が確認

することができるが、更に、クローズネットワーク２０内に、医師閲覧専用ＷＷＷサーバ６８とは別に、各地の調剤薬局の端末に接続された処方専用のＷＷＷサーバを設置しておき、医師が個人情報閲覧用の端末を利用して、医師閲覧専用ＷＷＷサーバ６８から、処方専用のＷＷＷサーバに処方箋を転送させると、処方専用のＷＷＷサーバから、患者が指定する特定の院外薬局へと、自動で処方箋（電子処方箋）が送付されるようにするとよい。

つまりこのようにすれば、電子処方箋を受信した院外薬局では、受信後、直ぐに薬剤の調合に取りかかることができ、その後訪れた患者に対して速やかに薬剤を渡すことができる。また、この場合、薬局窓口に利用者側端末１０を設置しておき、窓口に訪れた患者が、この利用者側端末１０に診察券兼用のＩＣカードを挿入することで、個人認証を行うようにすれば、調合した薬剤を間違いなく患者に渡すことができるようになる。

これによって、医療機関側は薬剤や処置の誤処方を回避することが出来るほか、院外処方で遠くなった、病院（医師）と薬剤師との距離を縮め、そのコミュニケーションの拡大と処方薬の精査が確実になり、認識の差異を縮めることで、あらゆるリスクを軽減できる。また、患者は、スムーズな診察で病院での待合い時間を短縮することができる他、院外処方薬局の窓口に訪れた直後に処方薬を受け取ることができる。また、患者は、従来のように発熱や嘔吐、腹痛といった症状があるにもかかわらず、その苦しみに耐えて薬剤が調合されるのを待つ、といった待合い時間がなくなることで、精神的、身体的負担を軽減することができる。

・応用例２…家庭と病院の双方向通信

また、上記第３実施例の健康管理システムにおいて、患者が自宅に設置した利用者側端末１０にＩＣカード１２を挿入して、利用者側端末１

０を専用ＷＷＷサーバ６に接続し、顧客情報変換サーバ３０にて個人認証を受けた後、医療機関に設置された医療機関専用ＷＷＷサーバにアクセスして、症状や処置、薬剤に関する質疑応答を、医師と双方向に行うことができるようにしてもよい。

そしてこのようにすれば、処方薬の中断や、来院指示を医師から患者に伝達することができる。つまり、この場合、患者は、初期段階の処置が重要な場合の症例や経過監視が必要な病状を医師に報告することで、翌日来院するよりも早く適切な指示を受けることができ、病状回復に大きく役立つ。

また、医師は、監視不可能な患者に対し、家庭での最も有効な処置を施すことが可能になることで、医師の治療方針に限りなく近い治療を行うことができるし、患者は、薬剤の取り扱いや、処置に困ったときに明確な答えを聞き出すことが可能となり、入院をしなくても医師と連携した効率の良い医療サービスを享受することができる。尚、このとき、翌回以降の受診予約ができるようにすると、患者にとって非常に便利である。

・応用例３…介護システム

上記第３実施例の健康管理システムにおいて、利用者が自宅に設置した利用者側端末１０にＩＣカード１２を挿入して、利用者側端末１０を専用ＷＷＷサーバ６に接続し、顧客情報変換サーバ３０にて個人認証を受けた後、介護サービスセンターに設置された専用のＷＷＷサーバにアクセスして、利用者個人の情報を送信できるようにしてもよい。

そして、この場合、特に、図１４に点線で示すように、利用者側端末１０に、音声認識装置とマイクロフォンとが組み込まれた音声入力装置１０ｂを接続し、利用者が、この音声入力装置１０ｂから所定の音声を入力することで、利用者側端末１０の起動（電源オン）や、専用ＷＷＷ

サーバ６から提供されるコンテンツメニューの変更、文字入力といった操作を、音声を使って入力可能できるようにすれば、体の不自由な利用者や老人層の利用者でも、簡単にまた不可なく介護サービスを受けることが可能になる。

また、この場合、上記応用例２に記載のように、病院や介護サービスセンターとの双方向通信ができるようにすれば、利用者とヘルパーとのコミュニケーションが容易に効率よく行われるようになり、急な体の変化や常日頃からの介護管理に有益なものとなる上、健康管理サーバのデータによって、長期の治療介護に大きな役割を果たすことができる。

また、このようにすれば、病院や看護サービスセンター側から、利用者の身体の状態に合わせて、食事のメニューや生活習慣、サイクルと言ったものを、随時指導することができるため、理想的な国民生活の健康状態の維持を図ることができる。

一方、こうした介護システムでは、緊急連絡システムを付加することで、独居老人や家族が外出中に一人になった老人若しくは要介護者が、健康状態の急変時に緊急救命要請を自動的に起動することができるようにすると非常に有益である。そして、この場合、特に、上述した第３実施例の健康管理用の個人情報データベースと連携することで、医師は、治療直前までの確実なバイタル等のデータを分析して、迅速に的確な対応を行うことができるようになり、救命率の向上につながる。

尚、こうした介護システムは、老人や要介護者に限らず、一般家庭にも導入することで、人間の生活における健康リスクの軽減に大きく貢献できる。

・応用例４…ニーズ対応システム

次に、第３実施例の健康管理システムにおいては、個人情報データベース６４に、利用者の個人情報として、バイタル測定器１０ａによる測

定データや医療機関での診療履歴等を記憶するものとしたが、例えば、個人情報データベース６４に、利用者の好みの食事メニュー、アレルギー反応データ、家の間取り、家庭への引き込み電力の状況、車や家の購入履歴、カタログ等の資料請求履歴、といった利用者のパーソナルライフデータを記憶するようにしてもよい。

そして、このようにすれば、飲食店や薬局、家具、家電、金融機関等のあらゆる店舗及び施設に、利用者側端末１０を設置することで、利用者が来店時に自己のＩＣカード１２を使用し、個人認証をすることで、必要なパーソナルライフデータを個人情報データベース６４から引き出し、これを店舗若しくは施設側で分析することによって、利用者に最適な商品を提供することが可能となる。

つまり、例えば、飲食店では、味付け、食材の大きさ、好みの堅さに至るまで調理方法を利用者好みに調節するとか、食材に利用者が食してはならない食物を使用しない、といったサービスを実現でき、薬局では、利用者が服用してはならない薬剤は販売しない、といったサービスを実現できる。

また、家具、家電店では、利用者の居宅の間取りに合わせた家具のサイズやデザインのフィッティング、新たな家電製品を追加することで、電力の総使用量の限界を超えないか否か、超えるのであれば、電力供給量を上げるようアドバイスを行ったり、電力会社に申し込みを行う、といったサービスを実現でき、金融機関等では、車や家の購買意欲の高い利用者に対し、ローンや保険をファイナンシャルプランニングサービスを付加して提案することで、利用者にとってより有利な商品を提供する、といったサービスを実現できる。

そして、こうしたニーズ対応システムを構築すれば、店舗及び施設の運営者は、従来にないより高品質なサービスを利用者に提供することが

可能になり、利用者のリピート率を飛躍的に向上させることができる。また、より効率的なマーケティングが可能になるため、従来より遙かに安いコストで売り上げを伸ばすことができる。

一方、利用者にとっては、従来以上に高品質なサービスを効率よく享受でき、便利になる上に、サービスの選択肢を、より自分のニーズに合うという見地で精査できることから、時間と生活費の無駄を省くことができるようになる。

・応用例５…ネット身分証明・身分保障

一方、本発明によれば、利用者の識別情報（上記各実施例における決済ＩＤ及び接続用暗号ＩＤ）と、利用者の住所、氏名、口座番号といった顧客情報とを区別し、インターネット等の広域ネットワーク上では、システム専用の識別情報（ＩＤ）のみを暗号化して伝送することで、セキュリティ性の高い個人認証を実現できることから、この個人認証機能を利用して、インターネット上での身分証明サービスを実現することもできる。

即ち、現在、インターネット上のＷＷＷサーバは、世界中に数え切れないほど存在するが、上記各実施例の顧客情報変換サーバを個人認証局とすることで、本発明のシステムの利用者（換言すれば登録者）が、世界中のどこのＷＷＷサーバに訪れても、本発明のシステムを利用して、身分証明を行うことができるようになり、ＷＷＷサーバーを利用した各種サービスの提供者及び利用者は、より価値の高いコンテンツの開発、提供、又は利用を行うことが可能になる。

そして、特に、サービス提供者は、利用者の身分が証明されていれば安心して商品の供給を行うことができるし、また、料金回収においてもより有利で個人に対する掛け売り等の選択肢を多数持つことができる。

また、利用者は、身分証明が持てることで、インターネット等の広域

ネットワーク上で、より効率的で安心なサービスを受けることができる他、支払い方法の選択肢を多数持つことができる。

また、身分を証明されれば、ネットワーク上で利用者の人権保護を行うことができるし、ネットワーク上での急な資金需要等にも、サービス提供者及び利用者の双方が対応できるようになり、実社会を含めたネットワーク関連の市場も急激に拡大し、経済発展にも貢献できる。また、インターネット等のネットワーク上での不正を軽減し、安全で有用なネットワークの発展を促すことができる。

また、このように本発明を利用して個人認証局を構築した場合、利用者の個人認証に対して保険を付加することで、ネットワーク上での利用者の身分保証をも行うことができるようになる。

・応用例６…リモート操作

一方、利用者が、携帯端末を利用して、外出先から本発明のシステムにアクセスすることで、顧客情報変換サーバ３０で個人認証を行った後、自宅や社内、施設の専用端末にアクセスできるようにすれば、利用者は、携帯端末をキーステーションとして、自宅や社内、施設内の多種の機器をリモート操作することもできるようになる。

つまり、この場合、帰宅時に快適な居住環境を実現できるようにするため、利用者は、例えば、エアコンのスイッチを入れたり切ったり、証明や水道を操作する、といったことを、外出先で、しかも安全に行うことができるようになる。また、利用者は、例えば、台所用品のコントロールによって、食材の下ごしらえや食事の準備を、外出先で行うこともできる。

また、本発明のシステムをこうしたリモート操作用に構築すれば、利用者は、自宅に居ながらにして、工場のライン等の様々な機器を制御することができるようになり、出勤の手間や費用、無駄な熱量の消費を抑

え、通勤に伴い事件・事故に遭遇する確率を軽減できる他、環境保全にも役立つ。

・応用例７…コンテンツ配信と課金

ところで、インターネット等の通信環境が整備されると、多様な商品やサービスの販売が可能になるが、特に、データのダウンロード等により販売される商品については、著作権や使用権等の問題があり、需要に対して市場の発展が伴っていない。しかし、本発明のシステムを利用すれば、こうした権利侵害のリスクを軽減することができる。

つまり、本発明のシステムを利用すれば、利用者側端末からインターネット上に送出される識別情報（ＩＤ）と顧客・暗号化情報データベースとを用いて、利用者個人を特定できることから、本発明のシステムを利用して、著作権や使用権等の問題がある商品（データ）を販売すれば、データの不正複製や転売等の防止につながる他、データのダウンロード時に即時に決済を行うことが可能となるため、料金の回収率が飛躍的に向上する。また、上述した応用例４のニーズ対応システムを利用することで、利用者好みのコンテンツを利用者個人毎に配信することが可能となり、これによって、市場の拡大を図ることができる。

またこの場合、利用者側端末にダウンロード専用の著作権保護システム付き記憶媒体を付加することで、著作権や使用権等に対する安全性をより向上することができる。尚、この場合、記憶媒体は、利用者によって自由に取り外しや入れ替えができるようにすることで、その記憶媒体を利用した他の機器でもダウンロードした商品を利用することが可能になり、利用者の利便性を向上させることができる。

・応用例８…利用者側端末

応用例３で説明したように、利用者側端末に、音声認識装置とマイクロフォンとからなる音声入力装置を装着すれば、利用者は、この音声入

力装置を利用して、利用者側端末を音声で操作することができるが、この音声入力装置（換言すれば音声認識システム）を利用すれば、利用者側端末での利用者の認証、或いは、顧客情報変換サーバでの利用者の認証を、音声データを利用して行うことが可能となる。

つまり、音声認識装置では、マイクロフォンから入力された音声の特徴パラメータを抽出し、予め登録された利用者の音声データと照合することで、利用者が入力した操作用の語彙を識別するが、音声認識装置で抽出された特徴パラメータから利用者の声紋データを生成して、これを個人認証用のデータとして利用すれば、個人認証を音声で行うことができる。

尚、顧客情報変換サーバでの利用者の認証を声紋データを用いて行う際には、声紋データを利用者側端末で暗号化し、これをネットワーク上に送出するようにすればよい。そして、この場合、暗号化された声紋データは、本発明の識別情報（上述したＩＤ）として利用することもできるし、識別情報に付与するパスワードとして利用することもできる。

また、利用者側端末には、コンパクトフラッシュや、ＳＤカード、メモリースティックといった、着脱自在な記憶媒体を使えるように、媒体用スロットを装備するとよい。つまり、こうすれば、利用者は、ネットワーク上で取得したデータを記憶媒体に記憶し、自由に利用できるようになる。尚、この場合、媒体用スロットとしては、ＰＣＭＣＩＡのＰＣカードスロットを装備して、あらゆる記憶媒体に対応させることが好ましい。

また、利用者側端末をテレビ用のセットトップボックスとし、デジタルビデオカメラやデジタルカメラ等からの出力信号を取り込み、テレビ用の映像・音声信号に変換して出力できるように構成すれば、インターネット等からダウンロードした画像データや動画データに加えて、これ

らのカメラで撮影した動画や静止画を、家庭内のテレビで再生することができるようになり、利用者側端末の用途を拡大できる。

また、このセットトップボックスに上述した媒体用スロットを実装すれば、家庭内のテレビで再生した各種画像を所望の記憶媒体に取り込むことができるようになり、その画像データを電子メールに添付して送信するといったことも容易に行うことができるようになり、利用者側端末の利用価値をより拡大することができる。

また、利用者側端末は、ケーブルテレビ用チューナやケーブルモデムと一体化することにより、家庭内の配線や機器の乱雑さを解消でき、しかも、ケーブルテレビのコンテンツ課金に第１、第２実施例の電子決済システムを利用することで、従来、ＣＡＴＶシステムでの課題とされた課金の問題を一気に解決できる。

・応用例９…教育システム

また次に、本発明によれば、顧客情報が漏洩することのない極めてセキュリティ性の高い情報処理システムを実現でき、しかも、利用者毎に提供する情報を設定できることから、例えば、利用者に対して教育用知的テキストを配信し、利用者からの質問等を受けて返信する、といった利用者毎の教育システムを実現することもできる。つまり、利用者の個人情報として、個人情報データベースに、利用者毎の学習履歴を蓄積し、その学習履歴の分析により、利用者に適した教育指導を行うのである。

そして、本発明によれば、顧客情報変換サーバで利用者を認証してから、次に利用者側端末を接続させるホームページを任意に切り替えることができるので、利用者側端末のファーストアクセスページを、その利用者の学習履歴等から分析した利用者に最適なページに設定（所謂カスタムコネクト）でき、初級クラスから上級クラスに至る迄のコンテンツ接続サービスを、利用者毎に最適な方法で自動で実現できる。

また、利用者のレベルが上がったときに、ファーストアクセスページを切り替えるために、利用者のＩＣカードや端末、パスワードやＩＤといったデータを変更する必要がないため、利用者にとって極めて使い勝手の良い教育システムを実現できる。

・応用例１０…ポータルサイトのフランチャイズ展開

また、本発明では、顧客情報変換サーバで利用者個人を特定した後、利用者側端末の接続先を任意に設定（カスタムコネクト）できることから、ポータルサイト（所謂インターネットの入り口）を、利用者毎に、サーバー側で自由にオペレーションできることになる。

そして、この機能を利用すれば、市町村といった地域毎に、ポータルサイトを設定し、市町村毎にポータル運営者を募り、本発明を広く国内で共用させることで、地域の情報革新は加速度的に進み、国内の情報化に貢献できるものになる。

そして、これらをより効率的に導入させるために、地域ポータルサイトの展開にフランチャイズシステムを導入すると、効率的にしかも地域毎にポリシーを築くことができ、地域情報を束縛しない形で情報提供が可能になり、利用者にとって非常に便利で、情報化推進にも大いに役立つことになる。

尚、以上の説明において、第１、第２実施例では電子決済システムを、第３実施例では健康管理システムを、応用例ではこれらを応用した各種システムを、夫々、独立したシステムとして個々に説明したが、本発明は、一つ若しくは地域毎に分散させた顧客情報変換サーバを利用することにより、上記各システムを統合した大規模な情報処理システムを容易に構築することができる。

産業上の利用可能性

以上詳述したように、本発明によれば、広域ネットワークを利用して利用者個人に対するサービスを行う情報処理システムにおいて、利用者個人の情報が漏洩するのを確実に防止し、当該システムを利用者が安心して利用できるという効果が得られる。

請求の範囲

1． 広域ネットワークを介して接続された利用者側端末から当該システムで提供可能なサービスの要求を受け付ける要求受付手段と、

該要求受付手段が利用者側端末からサービスの要求を受け付けると、該サービスを要求してきた利用者に対してサービスを提供するための情報処理を行う情報処理手段と、

を備えた広域ネットワーク用情報処理システムであって、

前記要求受付手段は、前記利用者側端末からサービスの要求を受けると、前記利用者側端末から、利用者を特定するために暗号化された識別情報を取得し、該識別情報を、利用者が要求してきたサービスを表す情報と共に、前記情報処理手段に送信し、

前記情報処理手段は、予め利用者毎に設定された顧客情報を記憶した顧客情報データベースを備え、前記要求受付手段から利用者の識別情報を受けると、該識別情報を解読して前記顧客情報データベースと照合することにより、サービスを要求してきた利用者が予め登録された顧客であるか否かを判断し、利用者が顧客である場合に、前記顧客情報データベースに登録された顧客情報に基づき、利用者が要求してきたサービスを実現するための情報処理を行うことを特徴とする広域ネットワーク用情報処理システム。

2． 前記要求受付手段は、前記利用者側端末から前記識別情報を取得する際、前記利用者側端末に対して、該識別情報と共に該識別情報に対応したパスワードを送信するよう要求し、該要求に応じて前記利用者側端末から送信されてきた識別情報及びパスワードを前記情報処理手段に転送し、

前記利用者側端末は、前記要求受付手段から前記識別情報及び前記パ

スワードの送信要求を受けると、利用者に対して前記識別情報に対応したパスワードの入力を要求し、該要求に応じて利用者が入力してきたパスワードと前記暗号化された識別情報とを前記要求受付手段に送信し、

前記情報処理手段は、前記要求受付手段から転送されてきた識別情報及びパスワードを前記顧客情報データベースと照合することにより、前記利用者が顧客であるか否かを判定することを特徴とする請求項１に記載の広域ネットワーク用情報処理システム。

３．　前記情報処理手段として、

前記顧客情報データベースを用いて得られる顧客情報に基づき、利用者から料金を徴収するための決済処理を行う決済手段、

を備え、前記要求受付手段は、前記利用者側端末からの要求に従い当該システムで実現可能な商取引のための情報を提供し、該情報提供の結果、前記利用者側端末から商取引のための決済要求を受けると、利用者から徴収すべき料金を表す料金情報を、前記利用者側端末から取得した識別情報と共に、前記決済手段に転送することを特徴とする請求項１又は請求項２に記載の広域ネットワーク用情報処理システム。

４．　前記決済手段は、前記顧客情報データベースに基づき利用者が予め登録された顧客であると判定すると、外部の信用調査用データベースに接続して該利用者の信用調査を行い、該信用調査の結果、該利用者は信用できると判定した場合にのみ、前記顧客情報に基づく決済処理を行い、該利用者は信用できないと判定すると、前記要求受付手段に対して該利用者との間の商取引を中止させることを特徴とする請求項３記載の広域ネットワーク用情報処理システム。

５．　前記決済手段は、利用者の口座から料金を徴収する外部の料金徴収システムに対して利用者及び徴収金額を表す情報を送信することにより、前記決済処理を外部の料金徴収システムを介して行うことを特徴と

する請求項３又は請求項４記載の広域ネットワーク用情報処理システム。

６．　当該広域ネットワーク用情報処理システムは、商品販売若しくは各種サービスを行う各種販売会社からの委託を受けて利用者との間で商取引を行う販売代行会社にて管理されるものであり、

前記要求受付手段は、前記決済手段にて利用者から料金を徴収可能であると判定されると、該利用者との間の商取引の結果を、対応する販売会社に通知することを特徴とする請求項３～請求項５の何れかに記載の広域ネットワーク用情報処理システム。

７．　前記要求受付手段は、利用者との間で商取引を行う販売会社にて管理され、

前記決済手段は、前記販売会社からの委託を受けて決済処理を行う決済代行会社にて管理されることを特徴とする請求項３～請求項５の何れかに記載の広域ネットワーク用情報処理システム。

８．　前記情報処理手段として、

前記顧客情報データベースを用いて得られる顧客情報に関連づけて利用者個人の個人情報が記憶された個人情報データベースを備え、前記要求受付手段を介して、前記顧客情報データベースに登録された顧客本人から個人情報の登録若しくは検索要求があると、該要求に従い前記個人情報データベースに登録された顧客本人の個人情報を更新若しくは検索する個人情報管理手段、

を備え、前記要求受付手段は、前記利用者側端末から前記個人情報の更新若しくは検索要求を受けると、該個人情報の更新若しくは検索要求を、前記利用者側端末から取得した識別情報と共に、前記個人情報管理手段に転送することを特徴とする請求項１～請求項７の何れかに記載の広域ネットワーク用情報処理システム。

９．　前記個人情報データベースに登録される個人情報は、顧客個人の

健康状態を表す情報であることを特徴とする請求項８記載の広域ネットワーク用情報処理システム。

１０．　前記個人情報管理手段は、

前記個人情報データベースに加えて、前記個人情報データベースに登録された個人情報を更新若しくは検索可能な利用者本人以外の者が前記顧客情報に関連付けて記憶された個人情報利用者データベースを備え、

前記要求受付手段を介して、前記顧客情報データベースに登録された顧客から他人の個人情報の更新若しくは検索要求があると、前記個人情報利用者データベースを参照して、前記個人情報の更新若しくは検索要求を行った顧客が更新若しくは検索可能な個人情報を抽出し、該抽出した個人情報に対する更新若しくは検索処理を行うことを特徴とする請求項８に記載の広域ネットワーク用情報処理システム。

１１．　前記個人情報データベースに登録される個人情報は、顧客個人の健康状態を表す情報であり、前記個人情報利用者データベースへの登録者は医師若しくは薬剤師であることを特徴とする請求項１０記載の広域ネットワーク用情報処理システム。

１２．　前記要求受付手段への接続を要求してきた利用者側端末から前記広域ネットワークを介して認証情報を取得し、該認証情報が予め登録された利用者のものであるときに、該利用者側端末と前記要求受付手段との通信を許可する認証手段、を備えたことを特徴とする請求項１～請求項１１の何れかに記載の広域ネットワーク用情報処理システム。

１３．　請求項１～請求項１１の何れかに記載の広域ネットワーク用情報処理システムにて前記利用者側端末として使用される端末装置であって、

前記暗号化された利用者の識別情報が記憶された記憶媒体を着脱自在に装着可能で、且つ、装着された記憶媒体から情報を読み取る情報読取

手段を備え、

前記要求受付手段から前記識別情報が要求されると、該情報を前記情報読取装置を介して前記記憶媒体から読み出し、前記広域ネットワークを介して前記要求受付手段に送信することを特徴とする端末装置。

１４．　請求項１２に記載の広域ネットワーク用情報処理システムにて前記利用者側端末として使用される端末装置であって、

前記認証情報及び前記暗号化された識別情報が記憶された記憶媒体を着脱自在に装着可能で、且つ、装着された記憶媒体から情報を読み取る情報読取手段を備え、前記認証手段又は前記要求受付手段から前記認証情報又は識別情報が要求されると、該情報を前記情報読取装置を介して前記記憶媒体から読み出し、前記広域ネットワークを介して前記認証手段又は前記要求受付手段に送信することを特徴とする端末装置。

１５．　前記記憶媒体には、前記情報に加えて前記広域ネットワークへの接続情報が記憶されており、当該端末装置は、前記記憶媒体から読み出した接続情報に基づき、当該利用者側端末を前記広域ネットワークに接続することを特徴とする請求項１３又は請求項１４記載の端末装置。

１６．　前記記憶媒体には、予めパスワードが設定されており、前記情報読取手段に前記記憶媒体が装着されると、利用者に対してパスワードの入力を要求し、該パスワードが設定されたものと不一致であるときには、前記要求受付手段への接続を禁止することを特徴とする請求項１３～請求項１５の何れかに記載の端末装置。

１７．　前記入力されたパスワードが設定されたものと不一致であることを所定回数連続して判定すると、前記記憶媒体を使用不能にすることを特徴とする請求項１６記載の端末装置。

１８．　前記記憶媒体には、予め利用者の指紋情報が記憶されており、当該端末装置は、前記情報読取手段に前記記憶媒体が装着されると、当

該端末装置に備えられた指紋センサを介して利用者の指紋を検出し、該検出結果と前記記憶媒体に記憶された指紋情報とから利用者の指紋が前記記憶媒体に登録された指紋情報と一致するか否かを判定し、不一致であるときには、前記要求受付手段への接続を禁止することを特徴とする請求項１３～請求項１７の何れかに記載の端末装置。

１９．　操作用のリモートコントロール装置を備え、前記指紋センサは、該リモートコントロール装置に組み込まれていることを特徴とする請求項１８記載の端末装置。

２０．　前記記憶媒体は、ＩＣカードからなり、当該端末装置は、前記情報読取手段としてＩＣカードリーダ／ライタを備えることを特徴とする請求項１３～請求項１９の何れかに記載の端末装置。

２１．　請求項１～請求項１２の何れかに記載の広域ネットワーク用情報処理システムにおいて、前記利用者側端末から前記広域ネットワークを介して前記要求受付手段に送信される識別情報の暗号化方法であって、

暗号化前の識別情報を、該識別情報を構成する文字、記号又は文字列からなる語句データに区分し、各語句データ毎に、予め作成された登録語句置換シートを用いて符号化すると共に、

該符号化した語句データを、各語句データ毎に、予め作成された乱数シートに記述された乱数を用いて所定データ長の暗号化データに変換し、該変換後の暗号化データを順に配置することにより、暗号化した識別情報を生成することを特徴とする決済用識別情報の暗号化方法。

２２．　前記登録語句置換シート及び前記乱数シートの少なくとも一方を、所定期間毎に更新し、前記暗号化した識別情報には、所定期間毎に更新される登録語句置換シート又は乱数シートの種別を表す種別情報を付与することを特徴とする請求項２１記載の決済用識別情報の暗号化方法。

２３．　前記請求項１～請求項１２の何れかに記載の広域ネットワーク用情報処理システムにおいて、前記情報処理手段が暗号化された識別情報を解読して利用者を特定するのに使用される暗号解読方法であって、

前記暗号化された識別情報を、所定データ長の暗号化データに区分し、各暗号化データ毎に、前記識別情報を暗号化した際に用いられた乱数シートに記述された乱数を用いて、符号化された語句データに変換すると共に、

該変換後の語句データを、更に、前記識別情報を暗号化した際に用いられた登録語句置換シートを用いて、暗号化前の識別情報を構成する文字、記号又は文字列からなる語句データに変換し、該変換後の語句データを順に配置することにより、暗号化前の識別情報を復元することを特徴とする暗号解読方法。

FIG. 1

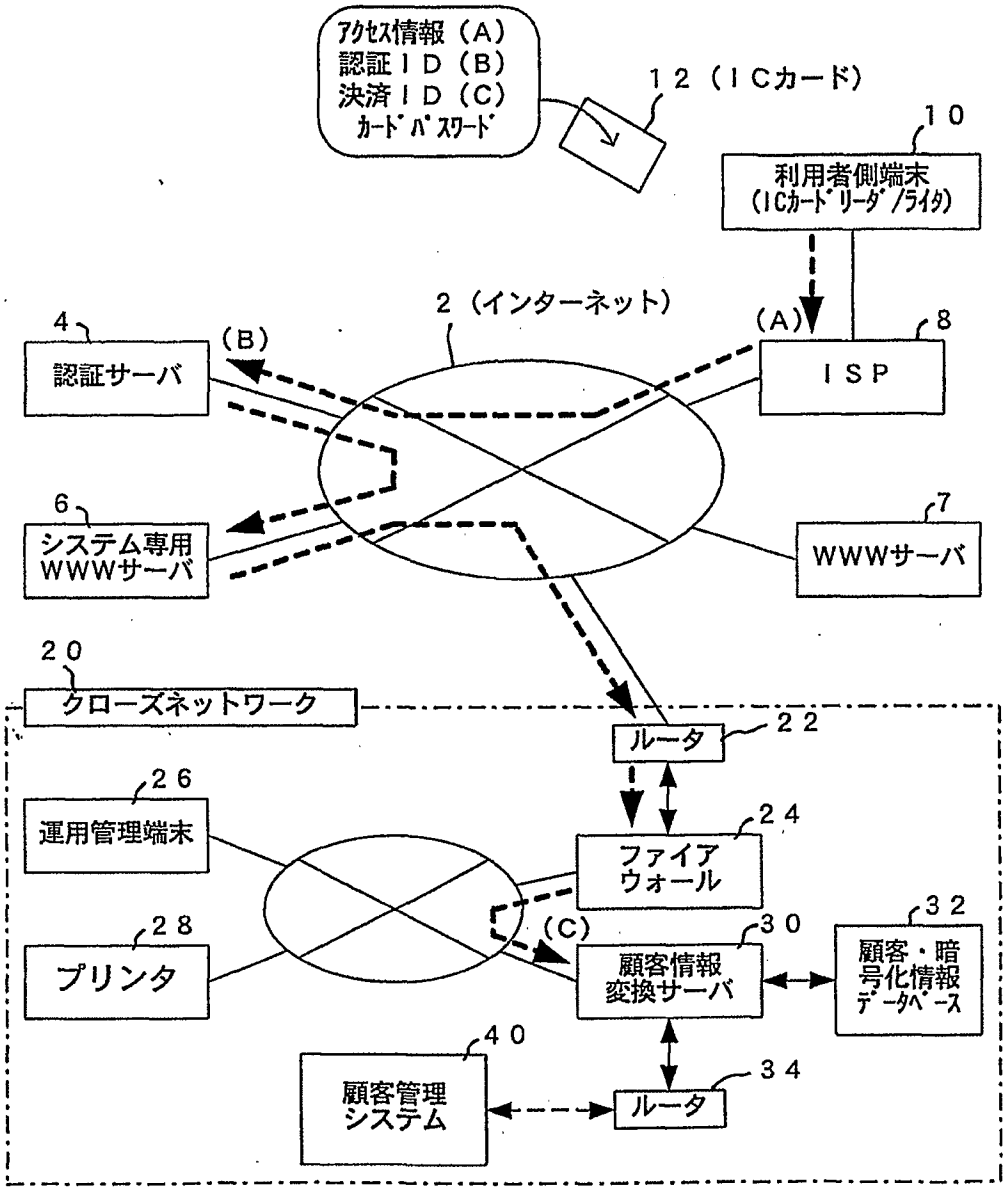

ｱｸｾｽ情報（A）
認証ＩＤ（B）
決済ＩＤ（C）
ｶｰﾄﾞﾊﾟｽﾜｰﾄﾞ
１２（ＩＣカード）
１０
利用者側端末
（ICｶｰﾄﾞﾘｰﾀﾞ/ﾗｲﾀ）
２（インターネット）
４
認証サーバ
（B）
（A）
８
ＩＳＰ
６
システム専用
WWWサーバ
７
WWWサーバ
２０
クローズネットワーク
ルータ
２２
２６
運用管理端末
２４
ファイア
ウォール
２８
プリンタ
（C）
３０
顧客情報
変換サーバ
３２
顧客・暗
号化情報
ﾃﾞｰﾀﾍﾞｰｽ
４０
顧客管理
システム
３４
ルータ

FIG. 2

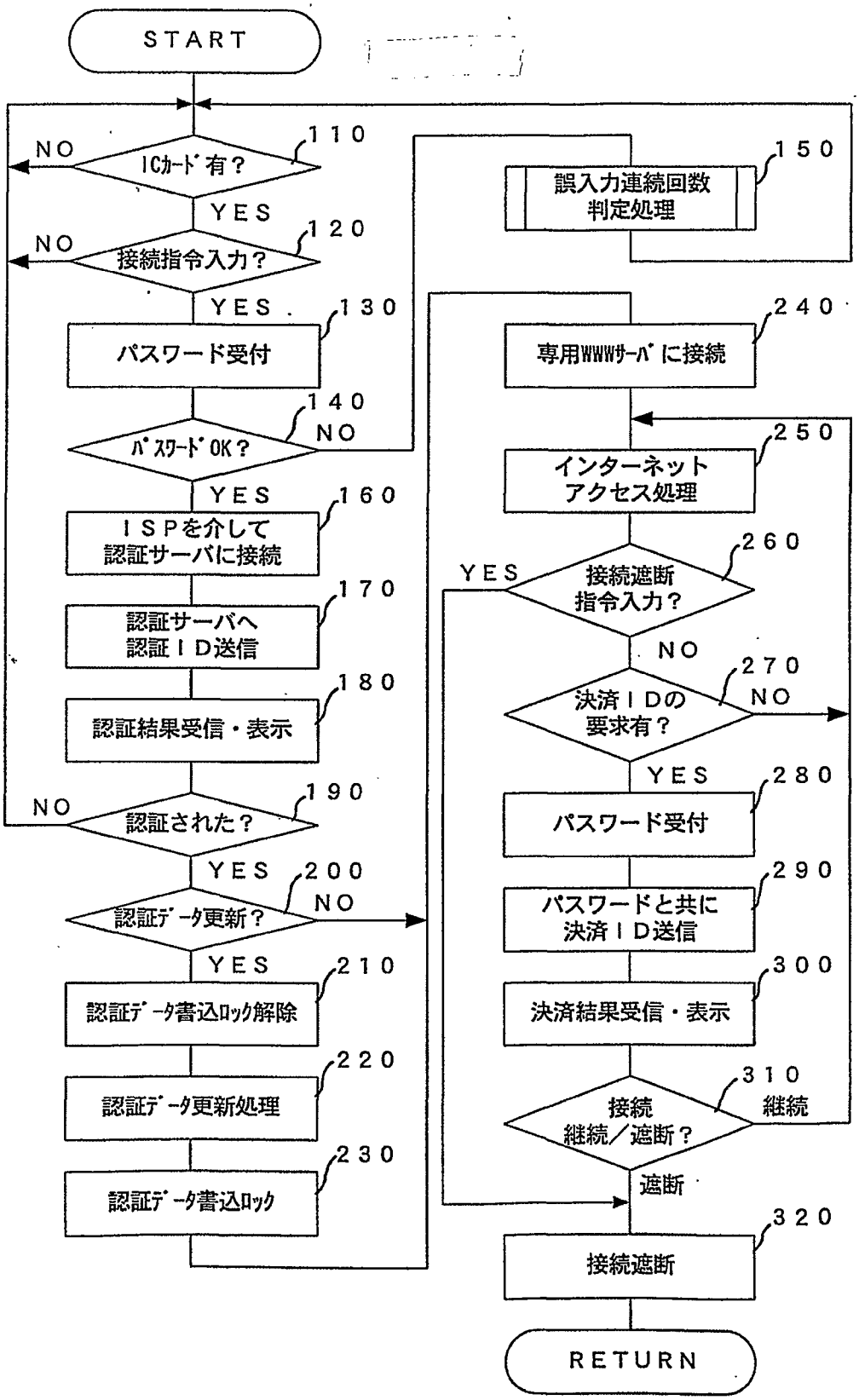

START
110
NO
ICカード有？
YES
120
NO
接続指令入力？
YES
130
パスワード受付
140
パスワードOK？
NO
YES
160
ＩＳＰを介して
認証サーバに接続
170
認証サーバへ
認証ＩＤ送信
180
認証結果受信・表示
190
NO
認証された？
YES
200
認証データ更新？
NO
YES
210
認証データ書込ロック解除
220
認証データ更新処理
230
認証データ書込ロック
150
誤入力連続回数
判定処理
240
専用WWWサーバに接続
250
インターネット
アクセス処理
260
YES
接続遮断
指令入力？
NO
270
決済ＩＤの
要求有？
NO
YES
280
パスワード受付
290
パスワードと共に
決済ＩＤ送信
300
決済結果受信・表示
310
接続
継続／遮断？
継続
遮断
320
接続遮断
RETURN

FIG. 3

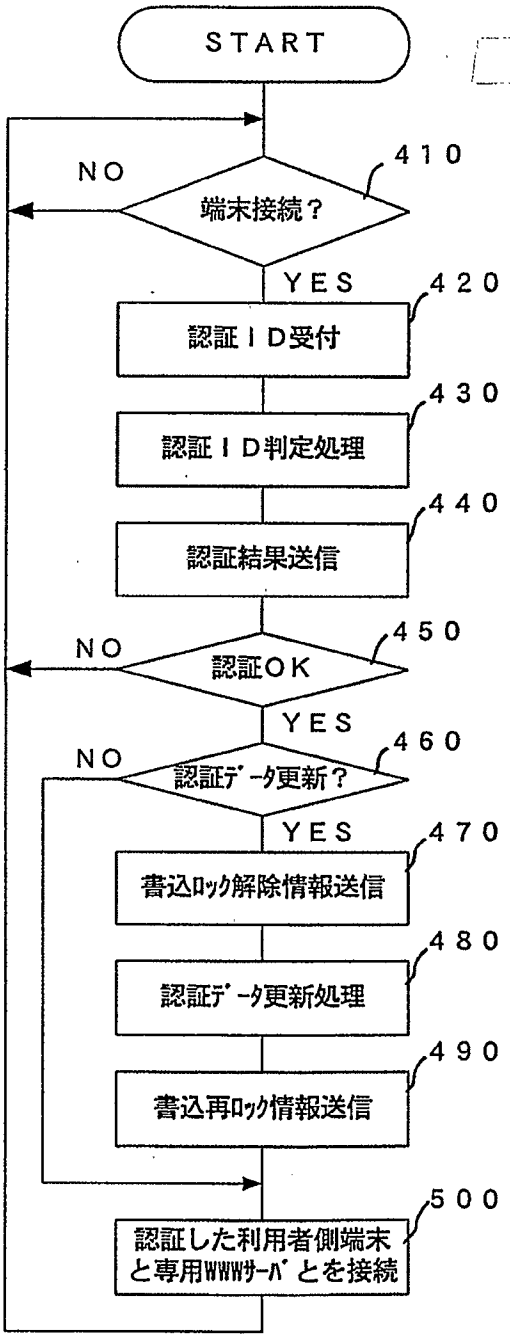

START
410
NO
端末接続？
YES
420
認証ＩＤ受付
430
認証ＩＤ判定処理
440
認証結果送信
450
NO
認証ＯＫ
YES
460
NO
認証ﾃﾞｰﾀ更新？
YES
470
書込ﾛｯｸ解除情報送信
480
認証ﾃﾞｰﾀ更新処理
490
書込再ﾛｯｸ情報送信
500
認証した利用者側端末と専用WWWｻｰﾊﾞとを接続

FIG. 4

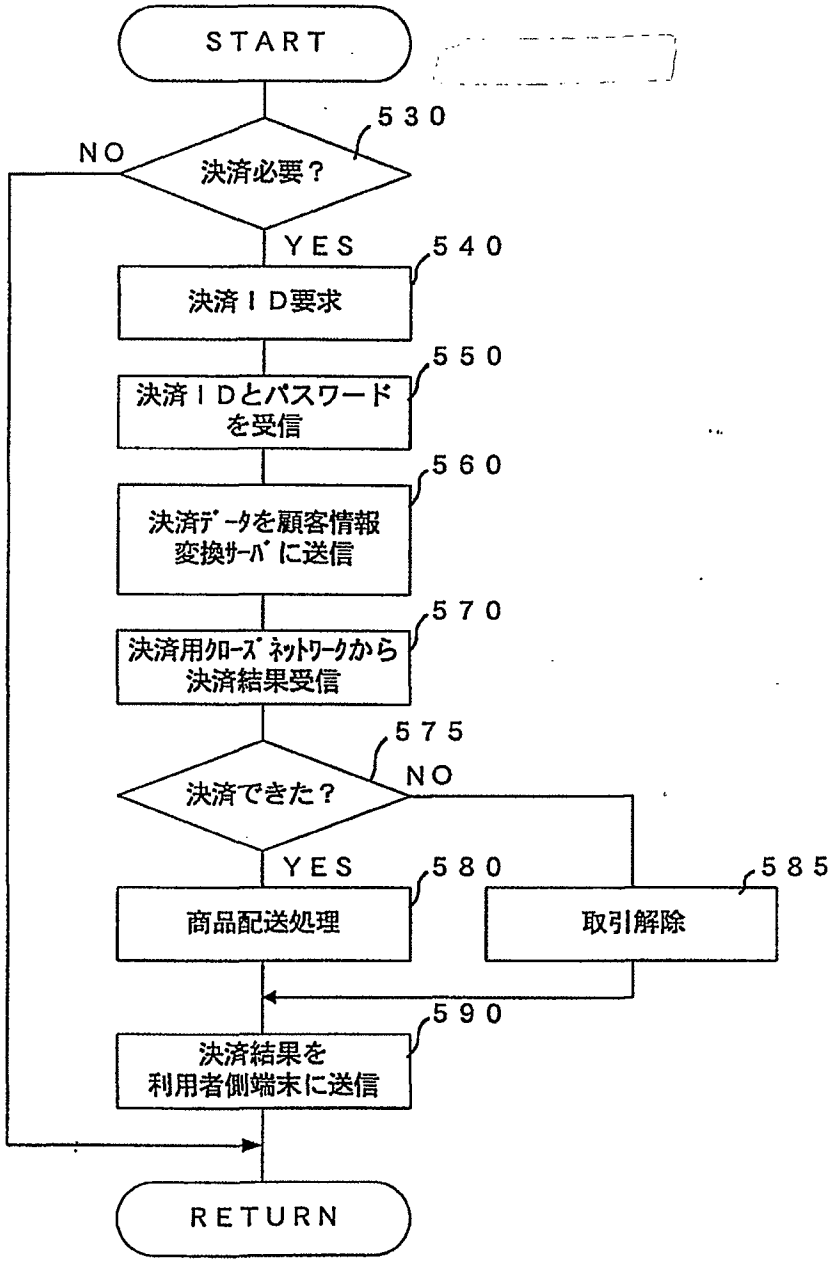

START
530
NO
決済必要？
YES
540
決済ＩＤ要求
550
決済ＩＤとパスワード
を受信
560
決済ﾃﾞｰﾀを顧客情報
変換ｻｰﾊﾞに送信
570
決済用ｸﾛｰｽﾞﾈｯﾄﾜｰｸから
決済結果受信
575
決済できた？
NO
YES
580
商品配送処理
585
取引解除
590
決済結果を
利用者側端末に送信
RETURN

FIG. 5

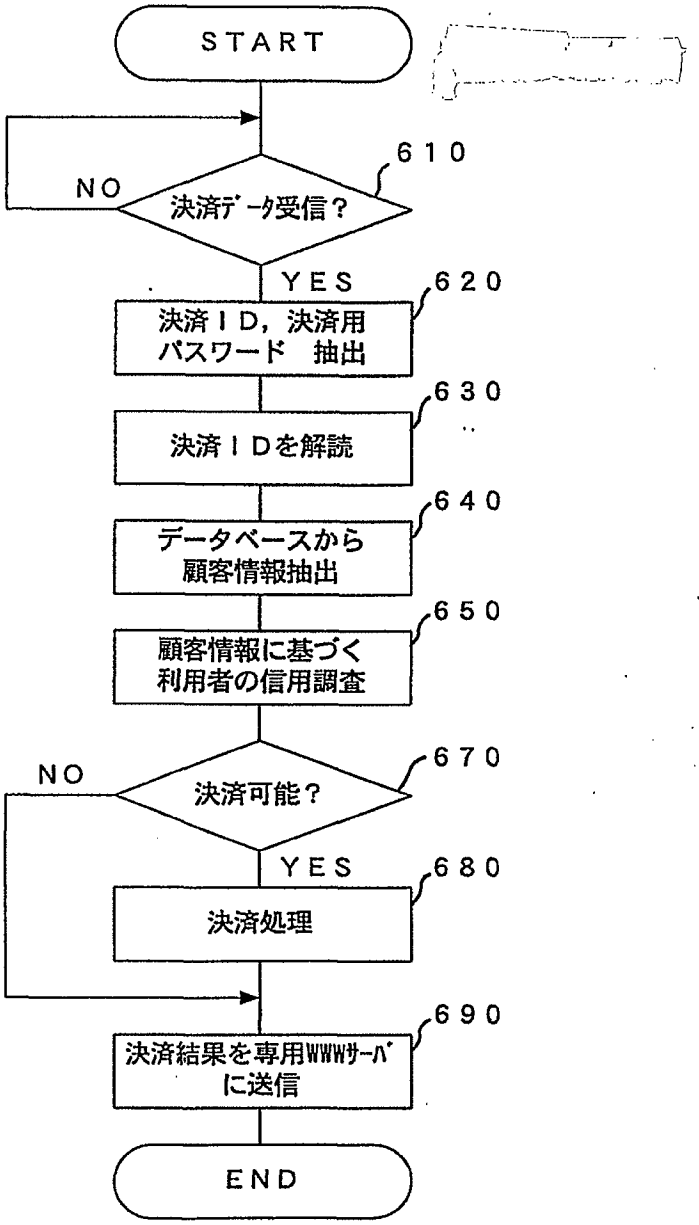

START
610
NO
決済データ受信？
YES
620
決済ＩＤ，決済用
パスワード　抽出
630
決済ＩＤを解読
640
データベースから
顧客情報抽出
650
顧客情報に基づく
利用者の信用調査
670
NO
決済可能？
YES
680
決済処理
690
決済結果を専用WWWサーバ
に送信
END

FIG. 6A

	00	01	02	03	・・・・	15
0	お	北海道	R	き	・・・・	な
1	S	A	か	和歌山	・・・・	ゆ
2	む	L	B	て	・・・・	宮崎
・	・	・	・	・		・
・	・	・	・	・		・
・	・	・	・	・		・
9	X	千葉	T	8	・・・・	1

FIG. 6B

識別符	00	01	02	03	・・・・	15
AS424	232	458	951	756	・・・・	864
AS545	142	588	846	684	・・・・	154
AS998	855	846	246	248	・・・・	612
AS914	926	052	823	987	・・・・	315

FIG. 6C

決済ＩＤ暗号化

乱数シート→	AS424	232	458	951	756	・・・	864
語句データ→		103	015	102	000	・・・	
ＩＤデータ→	AS424	139	443	859	756	・・・	

FIG. 6D

決済ＩＤ復号化

乱数シート→	AS424	232	458	951	756	・・・	864
ＩＤデータ→	AS424	139	443	859	756	・・・	
語句データ→		103	015	102	000	・・・	

決済ＩＤ → 和歌山 な か お

FIG. 7A

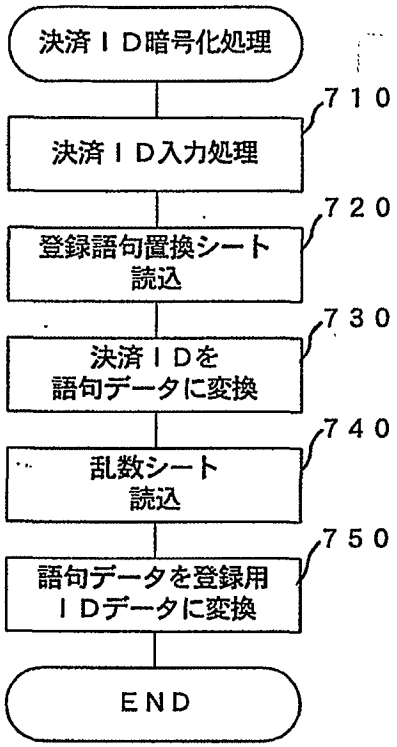

決済ＩＤ暗号化処理
７１０
決済ＩＤ入力処理
７２０
登録語句置換シート
読込
７３０
決済ＩＤを
語句データに変換
７４０
乱数シート
読込
７５０
語句データを登録用
ＩＤデータに変換
ＥＮＤ

FIG. 7B

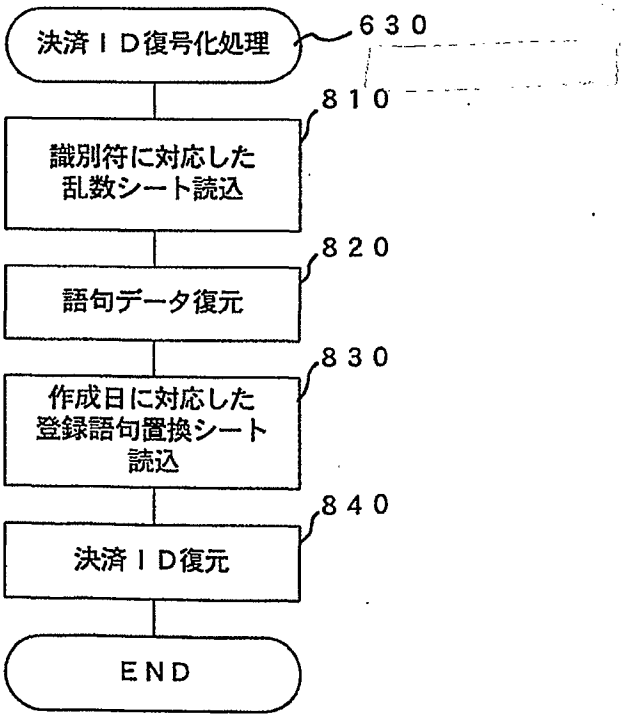

決済ＩＤ復号化処理
６３０
８１０
識別符に対応した
乱数シート読込
８２０
語句データ復元
８３０
作成日に対応した
登録語句置換シート
読込
８４０
決済ＩＤ復元
ＥＮＤ

FIG.8

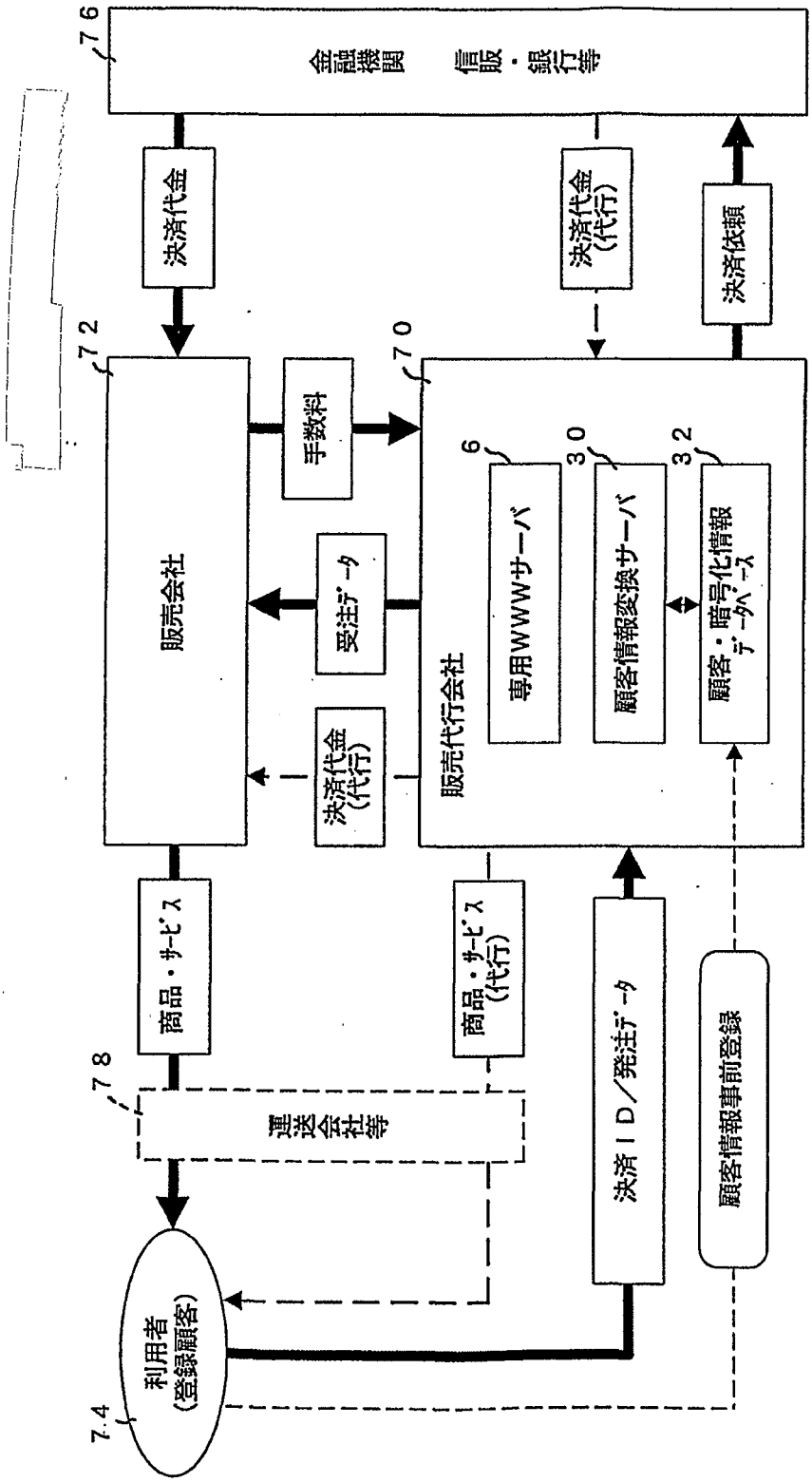

76
金融機関 信販・銀行等
決済代金
決済代金(代行)
決済依頼
72
70
販売会社
手数料
販売代行会社
6
専用WWWサーバ
30
顧客情報変換サーバ
32
顧客・暗号化情報データベース
受注データ
決済代金(代行)
商品・サービス
商品・サービス(代行)
決済ID／発注データ
顧客情報事前登録
78
運送会社等
利用者(登録顧客)
74

FIG. 9

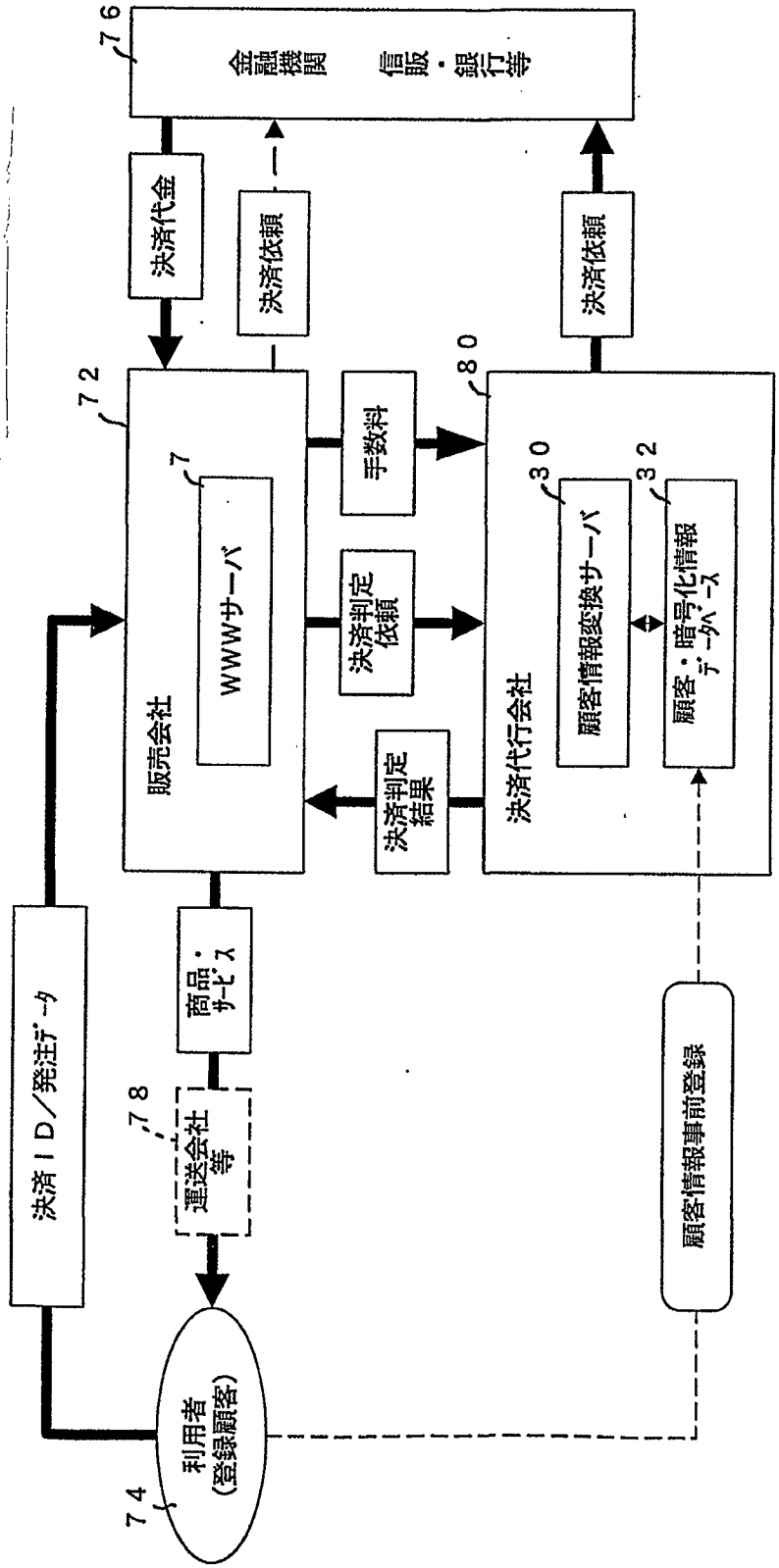

76
金融機関 信販・銀行等
決済代金
決済依頼
決済依頼
72
80
販売会社
WWWサーバ
7
手数料
決済判定依頼
決済判定結果
決済代行会社
30
顧客情報変換サーバ
32
顧客・暗号化情報データベース
決済ID／発注データ
商品・サービス
78
運送会社等
顧客情報事前登録
利用者（登録顧客）
74

FIG. 10

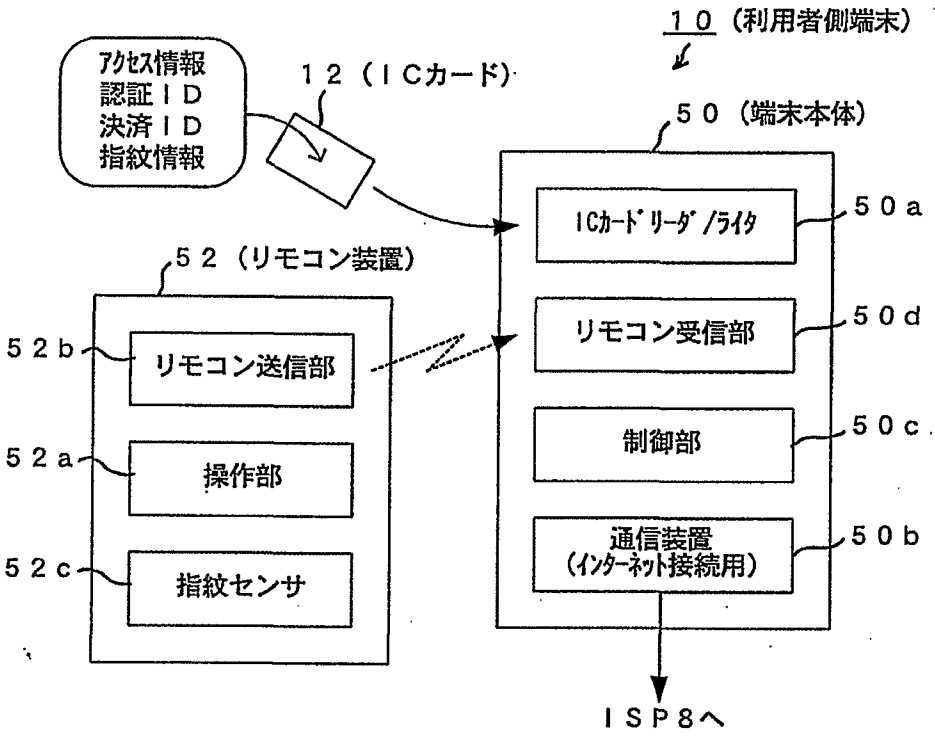

１０（利用者側端末）
アクセス情報
認証ＩＤ
決済ＩＤ
指紋情報
１２（ＩＣカード）
５０（端末本体）
ICカードリーダ/ライタ
５０ａ
５２（リモコン装置）
５２ｂ
リモコン送信部
リモコン受信部
５０ｄ
５２ａ
操作部
制御部
５０ｃ
５２ｃ
指紋センサ
通信装置
（インターネット接続用）
５０ｂ
ＩＳＰ８へ

FIG. 11

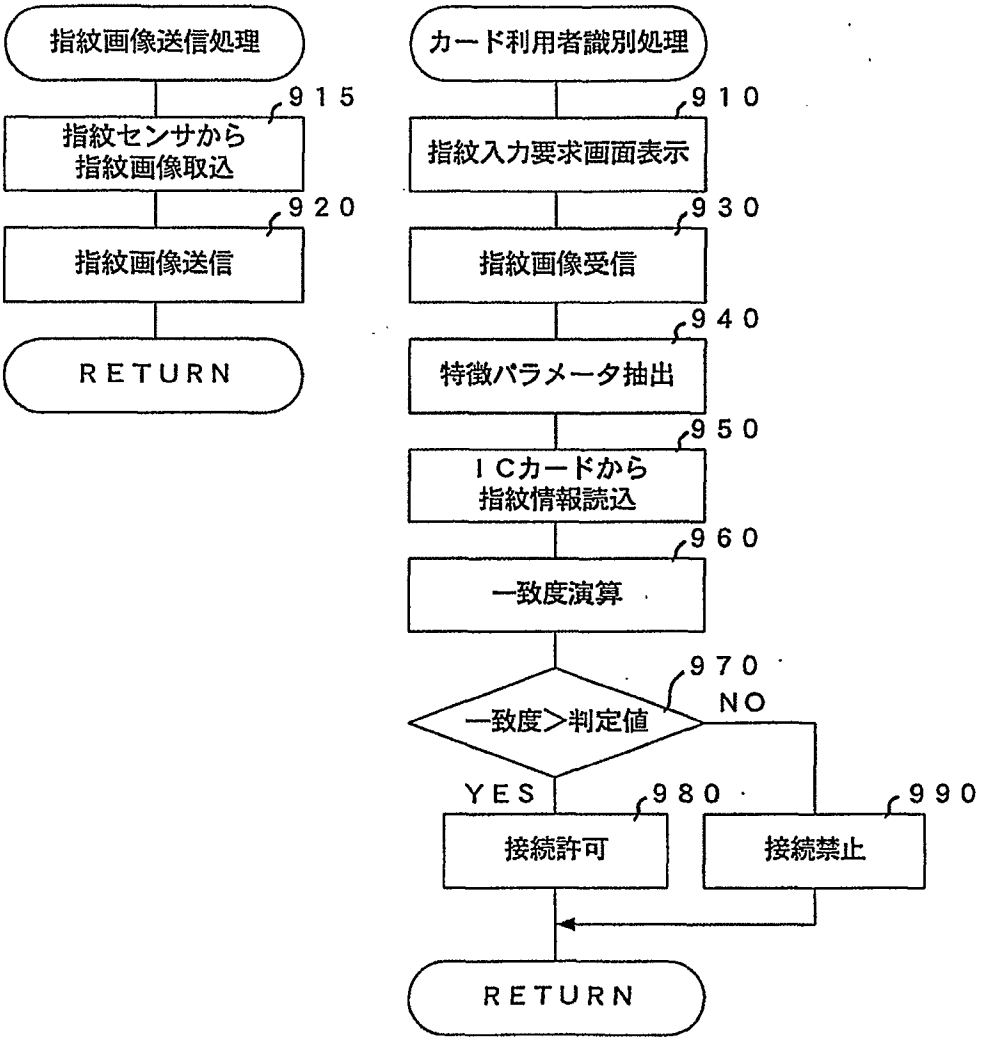

指紋画像送信処理
915
指紋センサから
指紋画像取込
920
指紋画像送信
RETURN
カード利用者識別処理
910
指紋入力要求画面表示
930
指紋画像受信
940
特徴パラメータ抽出
950
ICカードから
指紋情報読込
960
一致度演算
970
NO
一致度>判定値
YES
980
接続許可
990
接続禁止
RETURN

FIG. 12

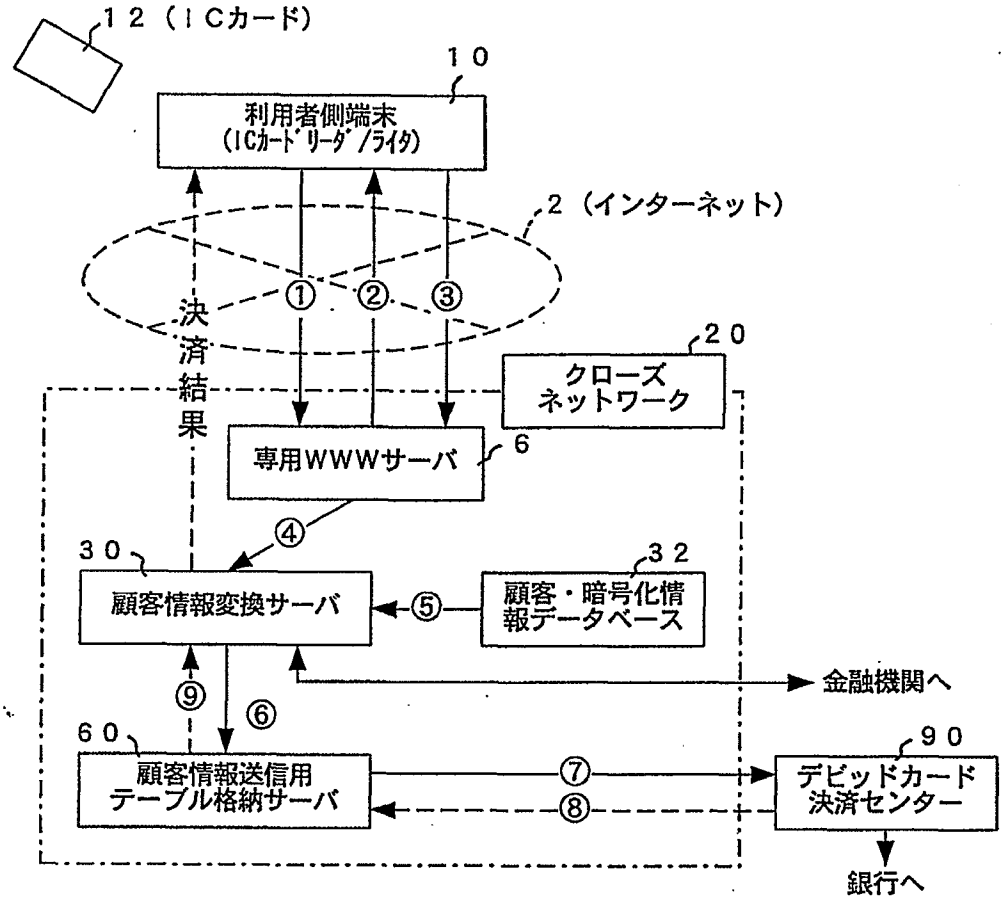

12（ICカード）
10
利用者側端末
(ICカードリーダ/ライタ)
2（インターネット）
①
②
③
決済結果
20
クローズネットワーク
専用WWWサーバ
6
④
30
顧客情報変換サーバ
⑤
32
顧客・暗号化情報データベース
金融機関へ
⑨
⑥
60
顧客情報送信用テーブル格納サーバ
⑦
⑧
90
デビッドカード決済センター
銀行へ

FIG. 13

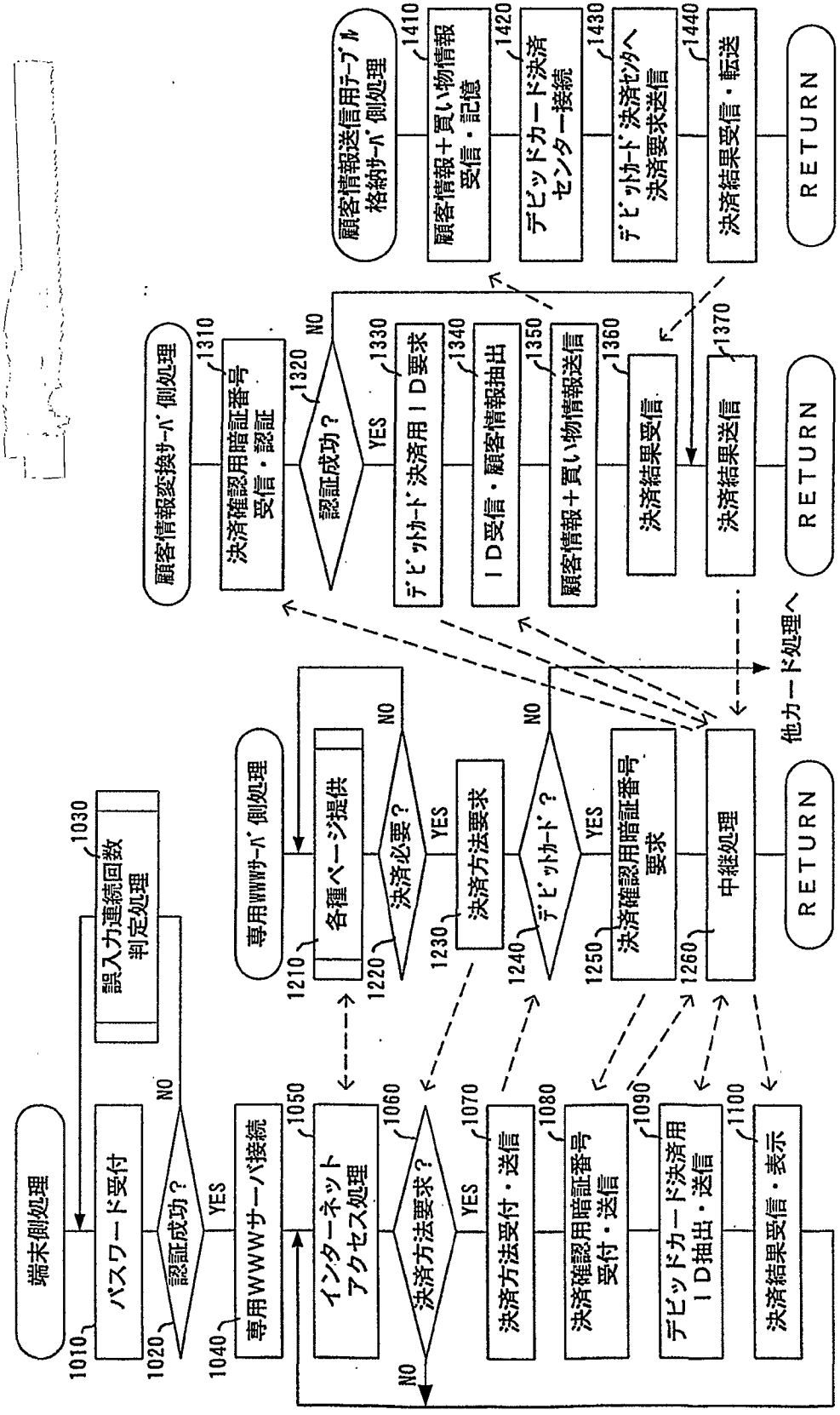

端末側処理
パスワード受付
誤入力連続回数判定処理
認証成功？
NO
YES
専用WWWサーバ接続
インターネットアクセス処理
決済方法要求？
決済方法受付・送信
決済確認用暗証番号受付・送信
デビットカード決済用ID抽出・送信
決済結果受信・表示
専用WWWサーバ側処理
各種ページ提供
決済必要？
決済方法要求
デビットカード？
決済確認用暗証番号要求
中継処理
RETURN
顧客情報変換サーバ側処理
決済確認用暗証番号受信・認証
認証成功？
デビットカード決済用ID要求
ID受信・顧客情報抽出
顧客情報＋買い物情報送信
決済結果受信
決済結果送信
他カード処理へ
顧客情報送信用テーブル格納サーバ側処理
顧客情報＋買い物情報受信・記憶
デビットカード決済センター接続
デビットカード決済センタへ決済要求送信
決済結果受信・転送
1010
1020
1030
1040
1050
1060
1070
1080
1090
1100
1210
1220
1230
1240
1250
1260
1310
1320
1330
1340
1350
1360
1370
1410
1420
1430
1440

FIG. 14

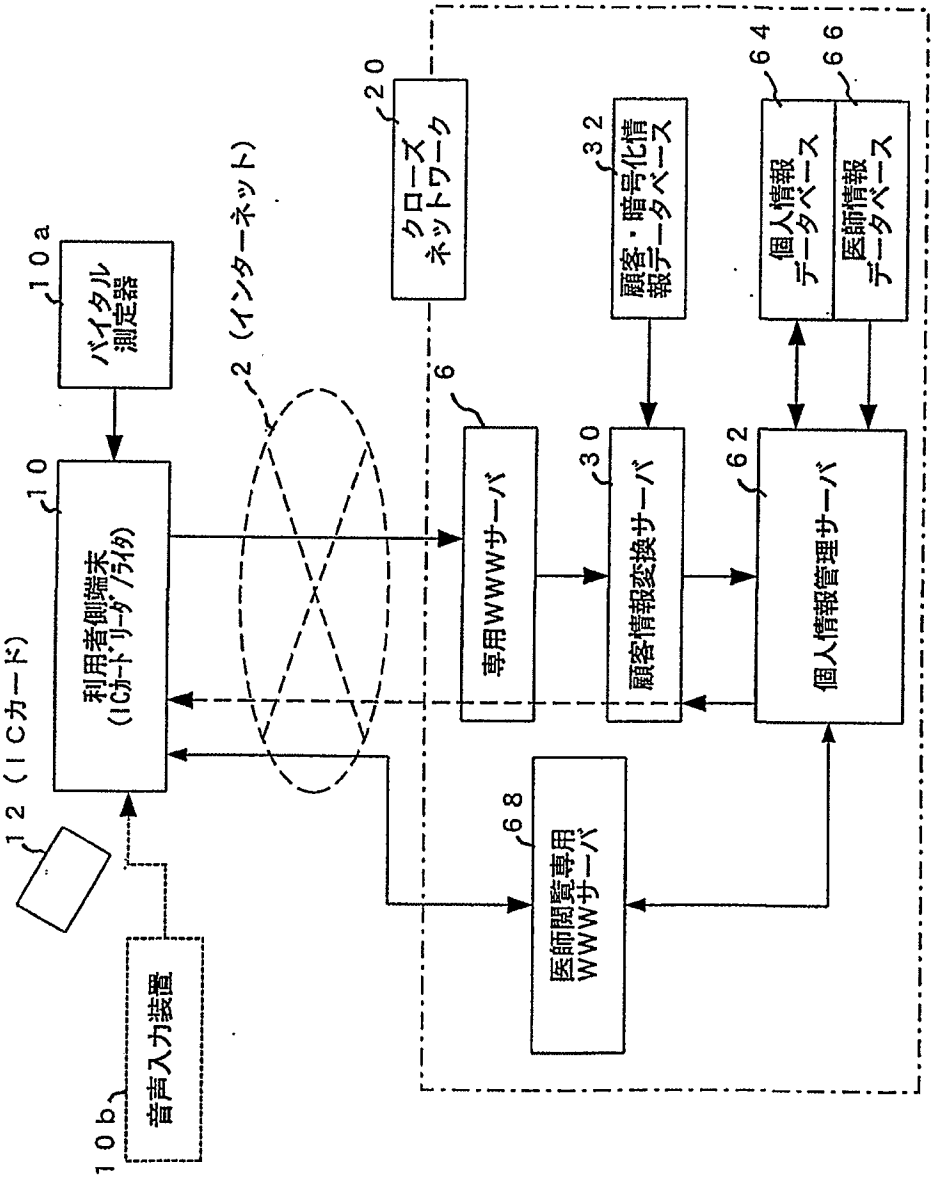

利用者側端末
(ICカードリーダ/ライタ)
10
バイタル
測定器
10a
音声入力装置
10b
12 (ICカード)
2 (インターネット)
クローズ
ネットワーク
20
専用WWWサーバ
6
顧客情報変換サーバ
30
顧客・暗号化情
報データベース
32
個人情報管理サーバ
62
個人情報
データベース
64
医師情報
データベース
66
医師閲覧専用
WWWサーバ
68

FIG. 15

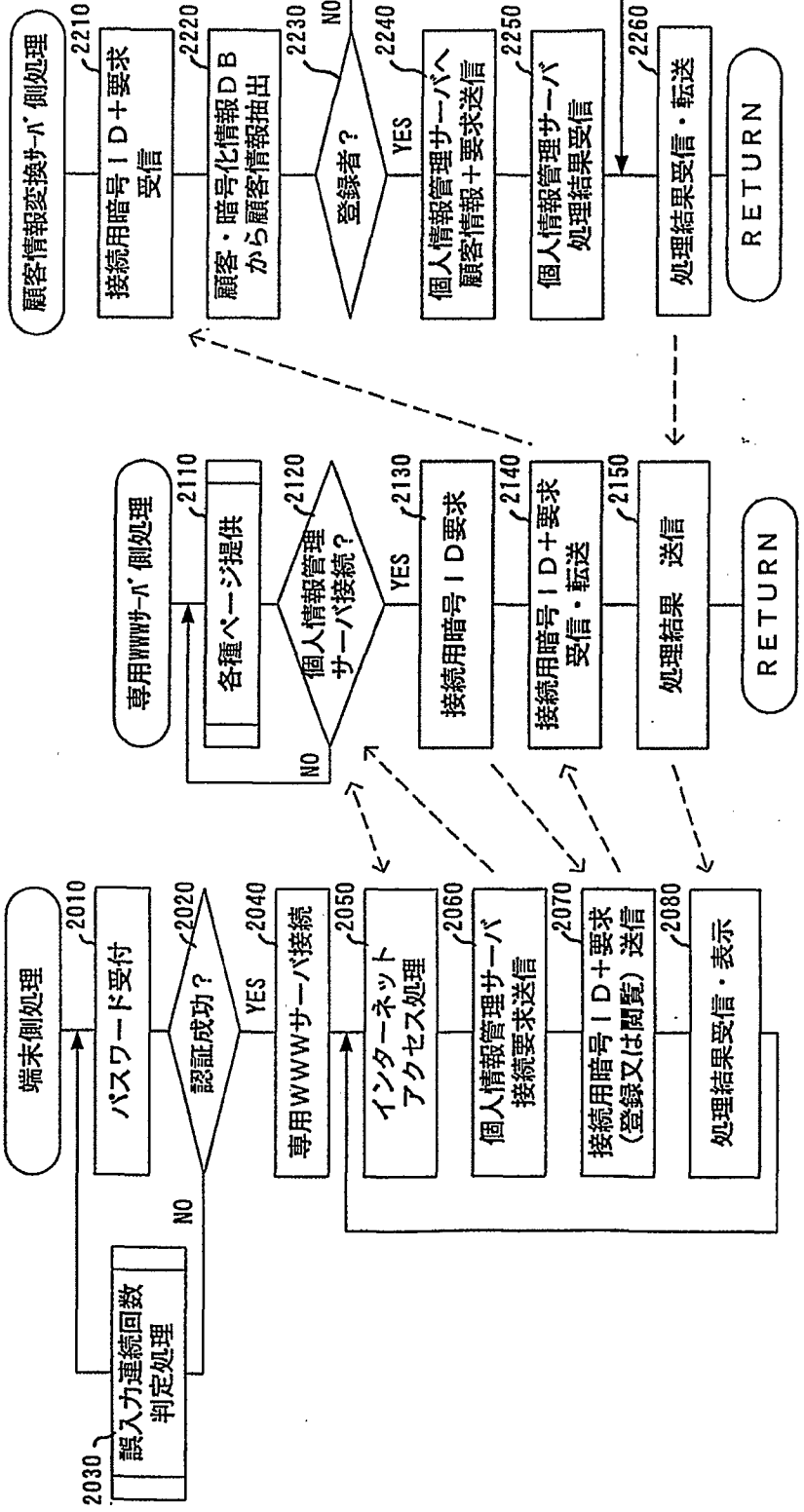
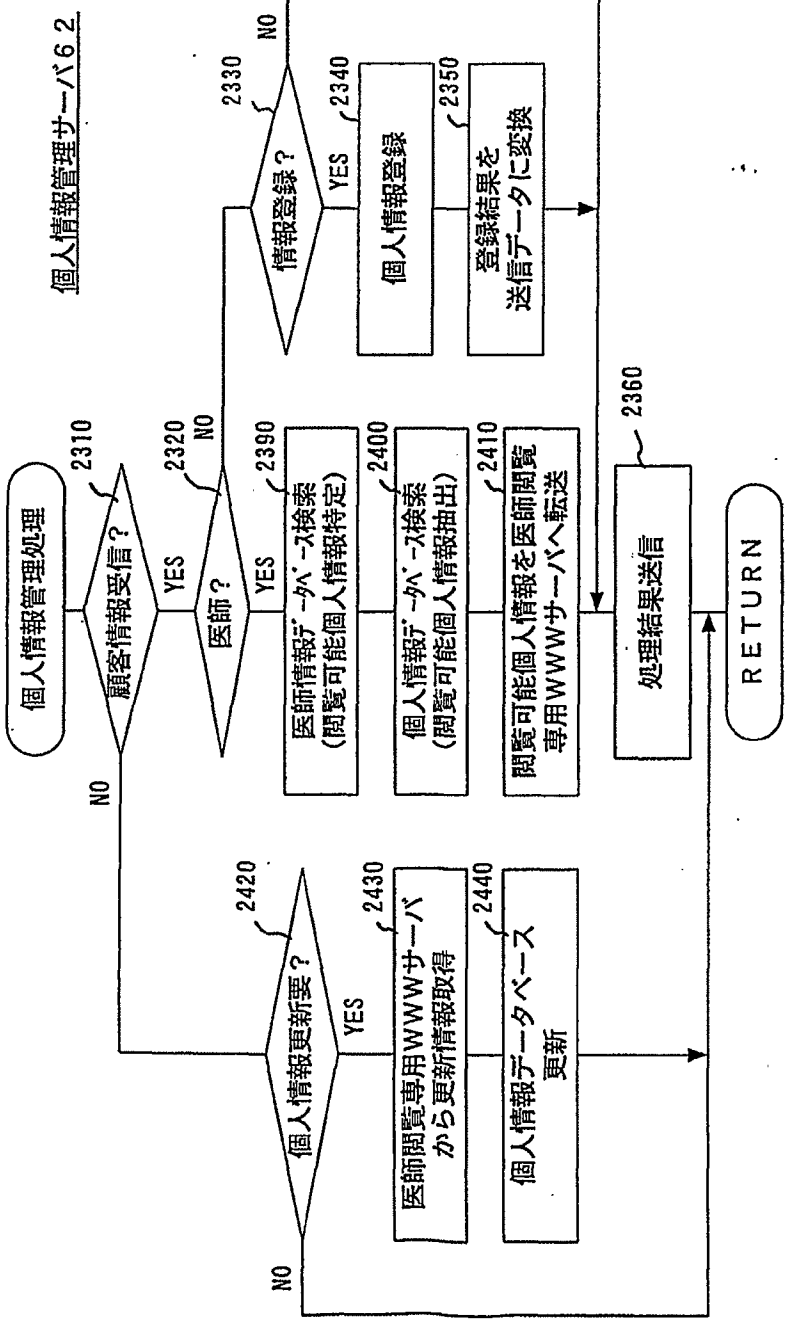

端末側処理
2010
パスワード受付
2020
認証成功？
YES
NO
2030
誤入力連続回数判定処理
2040
専用WWWサーバ接続
2050
インターネットアクセス処理
2060
個人情報管理サーバ接続要求送信
2070
接続用暗号ＩＤ＋要求（登録又は閲覧）送信
2080
処理結果受信・表示
専用WWWｻｰﾊﾞ側処理
2110
各種ページ提供
2120
個人情報管理サーバ接続？
YES
NO
2130
接続用暗号ＩＤ要求
2140
接続用暗号ＩＤ＋要求受信・転送
2150
処理結果　送信
RETURN
顧客情報変換ｻｰﾊﾞ側処理
2210
接続用暗号ＩＤ＋要求受信
2220
顧客・暗号化情報ＤＢから顧客情報抽出
2230
登録者？
YES
NO
2240
個人情報管理サーバへ顧客情報＋要求送信
2250
個人情報管理サーバ処理結果受信
2260
処理結果受信・転送
RETURN

FIG. 16


個人情報管理サーバ62
個人情報管理処理
2310
顧客情報受信？
YES
NO
2320
医師？
YES
NO
2330
情報登録？
YES
NO
2340
個人情報登録
2350
登録結果を送信データに変換
2370
個人情報データベース検索（個人情報抽出）
2380
抽出した個人情報を送信データに変換
2390
医師情報データベース検索（閲覧可能個人情報特定）
2400
個人情報データベース検索（閲覧可能個人情報抽出）
2410
閲覧可能個人情報を医師閲覧専用WWWサーバへ転送
2360
処理結果送信
RETURN
2420
個人情報更新要？
YES
NO
2430
医師閲覧専用WWWサーバから更新情報取得
2440
個人情報データベース更新

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/04717

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60, G09C1/00, H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60, G09C1/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 96/8783 A1 (First Virtual Holdings, Inc.), 21 March, 1996 (21.03.96), Full text & EP 791202 A1 & US 5826241 A & JP 10-508708 A	1-12 18,19,21-23
X		13-17,20
Y	JP 10-105614 A (Dainippon Printing Co., Ltd.), 24 April, 1998 (24.04.98), Full text (Family: none)	1-7
Y	JP 7-141442 A (Sanyo Electric Co., Ltd.), 02 June, 1995 (02.06.95), Full text (Family: none)	8-12
Y	JP 11-96363 A (Techno Imagica K.K.), 09 April, 1999 (09.04.99), Full text (Family: none)	18,19
Y	JP 11-203371 A (Nippon Conlux Co., Ltd.), 30 July, 1999 (30.07.99), Full text (Family: none)	21-23

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 July, 2001 (27.07.01)	07 August, 2001 (07.08.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/04717

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 11-17675 A (Fujitsu Limited), 22 January, 1999 (22.01.99), Full text & US 6199164 A	1-23
Y	Peter Wayner, translation: Hiroshi KAWAFUKU, "Digital Cash Technology", Softbank K.K., 20 May, 1997 (20.05.97), pages 75 to 91	1-23

国際調査報告

国際出願番号　PCT／JP01／04717

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　G06F17／60, G09C1／00, H04L9／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　G06F17／60, G09C1／00, H04L9／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO 96／8783 A1 (FIRST VIRTUAL HOLDINGS, INC.) 21. 3月. 1996 (21. 03. 96), 全文 & EP 791202 A1 & US 5826 241 A & JP 10－508708 A	1－12 18,19, 21－23
X		13－17, 20
Y	JP 10－105614 A (大日本印刷株式会社) 24. 4月. 1998 (24. 04. 98), 全文 (ファミリーなし)	1－7
Y	JP 7－141442 A (三洋電機株式会社) 2. 6月. 1995 (02. 06. 95), 全文 (ファミリーなし)	8－12

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日　27. 07. 01	国際調査報告の発送日　07.08.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 小山　満　5L　9458 電話番号　03－3581－1101　内線　3560

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP01／04717

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP　11－96363　A（テクノイマジカ株式会社）9．4月．1999（09．04．99），全文（ファミリーなし）	18,19
Y	JP　11－203371　A（株式会社日本コンラックス）30．7月．1999（30．07．99），全文（ファミリーなし）	21－23
A	JP　11－17675　A（富士通株式会社）22．1月．1999（22．01．99），全文　＆　US　6199164　A	1－23
Y	ピーター　ウェイナー著，川副博訳，デジタルキャッシュ　テクノロジー，ソフトバンク株式会社，20．5月．1997（20．05．97），p．75－91	1－23